DATASENSOR
value through detection
A DATALOGIC COMPANY

IndusLine®

UMTS Router

UR 5 and UR 5 SL

Benutzerhandbuch

www.tuv.com
TÜV
TÜV Rheinland Group
ID:9105030435

ISO 9001:2001 CE

Inhalt

1. Sicherheitshinweise 5
2. Beschreibung des UMTS Routers 6
    2.1. Einleitung 6
    2.2. UMTS Technologie 6
    2.3. HSDPA Tchnologie (High Speed Download Packet Access) 7
    2.4. Markierung der Lieferung 7
    2.5. Antennenanschluss 8
    2.6. SIM Kartenleser 9
    2.7. Stromversorgung 9
    2.8. Technische Parameter 10
    2.9. Beschreibung der einzelnen Routerteile 11
    2.9.1. UMTS Modul 11
    2.9.2. Steuerungsmikrocomputer 11
    2.10. Benutzerschnittstellen (Stecker) 12
        2.10.1. Belegung des PWR Stromversorgungssteckers 14
        2.10.2. Belegung des Steckers PORT1 – RS232 15
        2.10.3. Belegung des Steckers PORT1 - RS485 16
        2.10.4. Belegung des Steckers PORT1 – RS422 18
        2.10.5. Belegung des Steckers PORT1 - M-BUS 19
        2.10.6. Belegung des Steckers PORT1 - CNT 20
        2.10.7. Belegung des Steckers ETH 21
        2.10.8. Belegung des Steckers USB 22
    2.11. Technische Spezifikationen des Optionsanschlusses PORT1: 23
    2.12. Anzeige des Routerzustandes 25
    2.13. Inbetriebsetzung 25
    2.14. Mechanische und Einbauabmessungen sowie Empfehlungen zur Montage 26
3. Einsatz des Erweiterungsanschlusses 29
    3.1. Einsatz des Erweiterungsanschlusses des Routers UR 5 29
    3.2. Einsatz des Erweiterungsanschlusses des Routers UR 5 SL 31
4. Austausch der SIM Karten 33
    4.1. Austausch der zweiten SIM Karte beim Router UR 5 33
    4.2. Austausch der zweiten SIM Karte beim Router UR 5 SL 35
5. Einstellung der Konfiguration über den Webbrowser 37
    5.1. Netzinformationen 37
    5.2. DHCP Status 38
    5.3. IPsec Status 39
    5.4. UMTS/GPRS Status 39
    5.5. DynDNS Status 40
    5.6. System Log 40
    5.7. Konfiguration der Netzschnittstelle 41
    5.8. VRRP Konfiguration 44
    5.9. Konfiguration des Verbindungsaufbaus in UMTS/GPRS 45
    5.10. Firewall Konfiguration 48
    5.11. Konfiguration der Adressenübersetzung (NAT) 49
    5.12. Konfiguration des OpenVPN Tunnels 51
    5.13. Konfiguration des IPSec Tunnels 53
    5.14. Konfiguration des GRE Tunnels 55
    5.15. Konfiguration des L2TP Tunnels 57

5.16. Konfiguration des DynDNS Klienten 58
5.17. Konfiguration des NTP Klienten 59
5.18. Konfiguration des SNMP Agenten 59
5.19. Konfiguration und Versenden von SMS 61
5.20. Konfiguration des Erweiterungsanschlusses PORT1 66
5.21. Konfiguration des USB Anschlusses 67
5.22. Konfiguration des Startskripts 68
5.23. Konfiguration der automatischen Aktualisierung der Einstellungen 69
5.24. Änderung des Zutrittspasswortes 69
5.25. Einstellung der internen Uhr 70
5.26. Einstellung des SMS Zentrums 70
5.27. Erschließung der SIM Karte 70
5.28. Versenden einer SMS Nachricht 70
5.29. Erstellung der Sicherheitskopie der Konfiguration 71
5.30. Wiederherstellung der Konfiguration 71
5.31. Aktualisierung der Firmware 71
5.32. Restart 71
5.33. Standardeinstellung (Parameter des Herstellerwerkes) 72
5.33.1. LAN Configuration 72
5.33.2. VRRP Configuration 72
5.33.3. Firewall Configuration 72
5.33.4. UMTS/GPRS Configuration 73
5.33.5. NAT Configuration 73
5.33.6. OpenVPN Tunnel Configuration 74
5.33.7. IPsec Tunnel Configuration 75
5.33.8. GRE Tunnel Configuration 76
5.33.9. L2TP Tunnel Configuration 76
5.33.10. DynDNS Configuration 76
5.33.11. NTP Configuration 76
5.33.12. SNMP Configuration 77
5.33.13. SMS Configuration 77
5.33.14. Expansion Port Configuration 78
5.33.15. USB Port Configuration 78
5.33.16. Startup Script 79
5.33.17. Automatic Update 79
6. Einstellung der Konfiguration über Telnet 80
7. Mögliche Probleme 81
8. Literatur 81
9. FAQ (oft gestellte Fragen) 81
10. Kundenbetreuung 82
11. Hinweise zur Handhabung von elektrischem Abfall 83
12. Vorgehensweise bei Reklamationen 84
13. Garantieschein 87

Angewandte Symbole

Gefahr – wichtiger Hinweis, der die Sicherheit der Person oder die Funktionstüchtigkeit des Geräts beeinflussen kann.

Vorsicht – Hinweis auf mögliche Probleme, die in spezifischen Fällen auftreten können.

Information, Anmerkung – Informationen, die nützliche Ratschläge oder interessante Anmerkungen enthalten.

GPL Lizenz

Die Quellencodes, auf die sich die GPL Lizenz bezieht, können gebührenfrei nach der Zusendung des Antrags an die Anschrift info@conel.cz bezogen werden.

Conel s.r.o., Sokolská 71, 562 04 Ústi nad Orlicí, Tschechische Republik
Herausgegeben in der Tschechischen Republik, 31.8.2009

1. Sicherheitshinweise

Beachten Sie bitte folgende Hinweise:

- Der UMTS Router muss in Übereinstimmung mit sämtlichen gültigen internationalen sowie nationalen Gesetzen oder mit jeglichen speziellen, den Einsatz in vorgeschriebenen Anwendungen und Umgebungen regelnden Beschränkungen verwendet werden.
- Verwenden Sie nur für den Router bestimmtes Originalzubehör. Somit beugen Sie möglichen Gesundheitsschäden und Gerätebeschädigungen vor und stellen die Einhaltung aller einschlägigen Bestimmungen sicher. Nicht autorisierte Anpassungen oder Anwendung eines nicht zugelassenen Zubehörs können die Beschädigung des Routers sowie die Verletzung der gültigen Vorschriften zur Folge haben. Die Anwendung von nicht zugelassenen Anpassungen oder vom nicht zugelassenen Zubehör kann die Aufhebung der Garantiegültigkeit zur Folge haben.
- Der UMTS Router darf nicht geöffnet werden. Es ist nur der Austausch der SIM Karte erlaubt.

Vorsicht! Kleine Kinder könnten die SIM Karte verschlucken.

- Die Spannung auf dem Versorgungsstecker des Routers darf nicht überschritten werden.
- Setzen Sie den Router nicht extremen Umgebungsbedingungen aus. Schützen Sie das Gerät vor Staub, Feuchtigkeit und Hitze.
- Es wird empfohlen den Router nicht in der Nähe von Tankstellen zu benutzen. Wir weisen die Benutzer darauf hin, die Einschränkungen, die die Anwendung von Funkanlagen in Tankstellen, Chemiewerken oder bei Sprengungen betreffen, zu beachten.
- Bei Flugreisen schalten Sie den Router aus. Die Benutzung des Routers in Flugzeugen kann den Flugzeugbetrieb gefährden, das Mobilnetz stören und gesetzwidrig sein. Die Nichteinhaltung dieser Hinweise kann die Beanstandung oder Aufhebung der telefonischen Dienstleistungen bei diesem Kunden, rechtliche Schritte oder beiden dieser Möglichkeiten zur Folge haben.
- Bei der Anwendung des Routers in der Nähe von persönlichen medizinischen Geräten, wie z. B. Herzschrittmachern oder Hörgeräten, müssen Sie auf erhöhte Vorsicht achten.
- In der Nähe von Fernsehgeräten, Rundfunkgeräten und Personalcomputern kann der Router Störungen hervorrufen.
- Es ist empfohlen, dass Sie sich eine geeignete Kopie oder Sicherheitskopie der sämtlichen wichtigen im Speicher des Gerätes hinterlegten Einstellungen erzeugen lassen.

2. Beschreibung des UMTS Routers

2.1. *Einleitung*

Der UMTS Router ist ein kompaktes auf UMTS Modulbasis gebautes elektronisches Gerät, das Datenübertragungen mittels der Technologien HSDPA / UMTS / EDGE / GPRS ermöglicht.
Vor allem erweitert der Router die Möglichkeiten des UMTS Moduls um den Anschluss von mehreren PCs über eine eingebaute Ethernet-Schnittstelle. Darüber hinaus stellt die Router-Firmware den automatischen Aufbau und die Erhaltung der HSDPA / UMTS / EDGE / GPRS Verbindung sicher. Durch die Integrierung des DHCP Servers ermöglicht der Router den Benutzern eine einfache Installation und den Zutritt zum Internet.
Weiters ist der Router mit einer USB 2.0 Gastschnittstelle ausgestattet, die für den Anschluss von USB Geräten vorgesehen ist.
Auf Kundenwunsch ist es möglich, den Router mit Portmodul PORT1 auszustatten und somit die Funktionstüchtigkeit des Geräts zu erweitern. Auf diese Weise kann der Router mit der seriellen Schnittstelle RS232, RS485/RS422, M-BUS oder mit dem CNT (E/A Modul) ergänzt werden.
Den UMTS Router gibt es in zwei Varianten. Die Grundversion des Routers ist UR 5, die Version UR 5 SL ist die Grundversion des Routers mit einem Aluminiumgehäuse. Die beide Versionen des Routers nutzen die gleiche Firmware.

Beispiele für mögliche Anwendungen

- Fernwartung
- Steuerung des Fahrzeugparks
- Sicherheitssysteme
- Telematik
- Telemetrie
- mobiles Büro
- Verkaufs- und Ausgabeautomaten

2.2. *UMTS Technologie*

Fur den Funkteil von UMTS (Universal Mobile Telecommunication System), der als UTRA (UMTS Terrestrial Radio Access) bezeichnet wird, ist ein Frequenzbereich von 155 MHz im Frequenzbereich um 2 GHz eingeräumt. Es handelt sich um die Bänder 1900–1980 MHz, 2010–2025 MHz und 2110–2170 MHz.
Dem UMTS System wurde die Codeabtrennung der übertragenen Kanäle zugrunde gelegt – das System benutzt die Zutrittmethode WCDMA (Wideband Code Division Multiple Access – Breitbereichsystem CDMA). WCDMA nutzt die direkte Spektrumausbreitung (Direct Spread) aus. Zur Übertragung nutzen die UMTS Netze zwei Duplextechniken – Übertragungsmodi – aus, FDD (Frequency Division Duplex), wobei die Frequenzabtrennung des Kanals (d. h. Uplink und Downlink verwenden einen unterschiedlichen Kanal) dieser Technik zugrunde liegt, und TDD (Time Division Duplex), wobei die Zeittrennung (d. h. Uplink und Downlink benutzen einen Kanal, in dem sich die beiden Richtungen in der Zeit wechseln) dieser Technik zugrunde liegt.

Das UMTS Netz besteht aus drei grundlegenden Komplexeinheiten:

- Grundnetz CN (Core Network) – eigener Kern des UMTS Netzes,
- UTRAN Netz (UMTS Terrestrial Radio Access Network) – Rundfunkzutrittsnetz,
- Anwenderteil UE (User Equipment) – eine, dem Benutzer den Zutritt in das UMTS Netz ermöglichende Komplexeinheit.

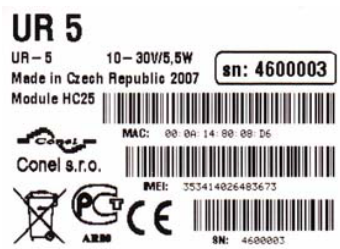
2.3. HSDPA Tchnologie (High Speed Download Packet Access)

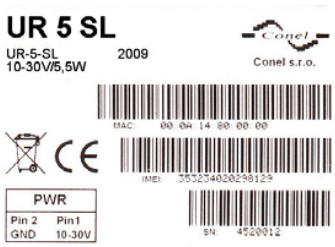
Es handelt sich um die verbesserte und erweiterte Version von UMTS-TDD. HSDPA ist sowohl für UMTS FDD als auch für UMTS TDD erreichbar. HSDPA erhöht auf eine wesentliche Weise die Übertragungsgeschwindigkeit des Downlink. Dies erzielt man auf der Programmebene. Somit werden die Kapazitäten der BTS Stationen und der Basisrundfunkstation verdoppelt, damit wird die Möglichkeit gegeben, die Daten und das Signal von mehreren Benutzern gleichzeitig zu bearbeiten. Der HSDPA Technologie liegen einige Innovationen der Netzarchitektur zugrunde, dank denen die niedrigere Verzögerung, schnellere Reaktionen auf Änderung der Kanalqualität und schnellere Bearbeitungen von HARQ, also Hybid Automatic Repeat Request, von der automatischen Hybridanforderung auf Wiederholung der Übertragung erreicht wird. Der Transportkanal für HSDPA nutzt die erreichbaren Frequenzen, auf denen er die Daten gemeinsam in Paketen überträgt, wirksam aus. Mittels bestimmter Algorithmen werden diese Pakete anschließend unter die einzelnen Benutzer aufgeteilt.

2.4. Markierung der Lieferung

Schildmuster:

Handelsbezeichnung	Typenbezeichnung	Sonstiges
UR 5	UR-5	Grundversion
UR 5 SL	UR-5-SL	Version mit Aluminiumgehäuse

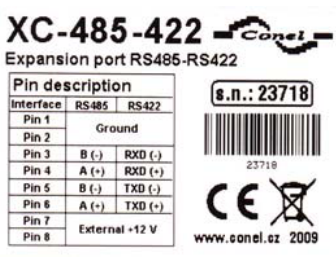


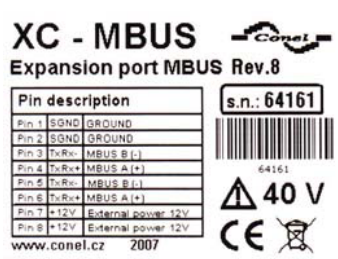


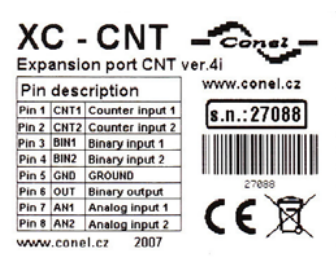
Schildmuster des Optionsanschlusses PORT1:

Handelsbezeichnung	Typenbezeichnung	Stromversorgung
Expansion port RS232	XC-232	Interne Stromversorgung
Expansion port RS485-RS422	XC-485422	Interne/Externe Stromversorgung
Expansion port MBUS	XC-MBUS	Externe Stromversorgung
Expansion port CNT	XC-CNT	Interne Stromversorgung

XC - 232
Expansion port RS232
Pin description
s.n.: 22646
Pin 1 RTS Request To Send
Pin 2 CTS Clear To Send
Pin 3 DTR Data Terminal Ready
Pin 4 DSR Data Set Ready
Pin 5 GND GROUND
Pin 6 RXD Receive Data
Pin 7 CD Carrier Detect
Pin 8 TXD Transmit Data
www.conel.cz 2007




XC - MBUS
Expansion port MBUS Rev.8
Pin description
Pin 1 SGND GROUND
Pin 2 SGND GROUND
Pin 3 TxRx- MBUS B (-)
Pin 4 TxRx+ MBUS A (+)
Pin 5 TxRx- MBUS B (-)
Pin 6 TxRx+ MBUS A (+)
Pin 7 +12V External power 12V
Pin 8 +12V External power 12V
s.n.: 64161
40 V
www.conel.cz 2007


XC - CNT
Expansion port CNT ver.4i
www.conel.cz
Pin description
Pin 1 CNT1 Counter input 1
Pin 2 CNT2 Counter input 2
Pin 3 BIN1 Binary input 1
Pin 4 BIN2 Binary input 2
Pin 5 GND GROUND
Pin 6 OUT Binary output
Pin 7 AN1 Analog input 1
Pin 8 AN2 Analog input 2
s.n.: 27088
www.conel.cz 2007

Der Standardtyp des Gerätes enthält im Lieferumfang:

- eigenen UMTS Router,
- Netzteil,
- UTP kabel, querverdrahtet,
- externe Antenne,
- Kunststoffelemente zur Befestigung auf der DIN Schiene mit Befestigungsschrauben,
- Installations-CD mit Anleitung.

Zum Standardtyp kann weiteres Zubehör bestellt werden:

• Erweiterungsanschluss RS232, RS485/422, MBUS oder CNT (die den Abstand haltende Säulen sind im Lieferumfang enthalten),
• Adapter zur Anwendung von zweiten SIM Karte.

Der Router ist vorgesehen:

- zur Montage auf die Montageplatte mithilfe von Durchgangsbohrungen (nur die Versi on UR 5),
- beziehungsweise zum Auflegen auf die Arbeitsfläche,
- bei der Montage auf die DIN Schiene ist es notwendig Kunststoffelemente zu verwen- den (sind im Standardlieferumfang nicht enthalten).

2.5. *Antennenanschluss*

Die externe Stabantenne wird an den Router über den FME Stecker auf der Rückplatte angeschlossen.
Beispiel für eine Antenne:

2.6. *SIM Kartenleser*

Auf der Frontplatte des Routers, beziehungsweise im Innenraum des Routers, falls ein Adapter für die zweite SIM Karte vorhanden ist, wird der SIM Kartenleser zum Lesen der SIM Karten 3 V und 1,8 V untergebracht. Zur Inbetriebnahme des Routers ist es notwendig, die aktivierte SIM Karte mit entsperrtem PIN Code in den Kartenleser einzulegen. Die SIM Karten können unterschiedlich eingestellte APN (Access Point Name) haben.

2.7. *Stromversorgung*

Router braucht eine Gleichstromversorgung +10 bis +30 V. Router hat einen eingebauten Schutz gegen Verpolung ohne Anzeige.
Beim Empfang beträgt der Verbrauch 1 W. Bei Datensendung beträgt der Wert des Spitzenverbrauchs 5,5 W. Für die richtige Funktion ist es notwendig, dass das Netzteil für Stromversorgung imstande ist, Spitzenstrom von 600 mA zu liefern.

HSDPA/UMTS/EDGE/GPRS Modul		UR5 UR5 SL
Entspricht den Normen		EN 301 511, v9.0.2 , EN 301 908-1&2 V2.2.1, ETSI EN 301 489-1 V1.6. 1, EN 60950-1:06 ed.2
GPRS Parameter		GPRS Multislot Klasse 10, CS 1 to 4 EGPRS Multislot Klasse 10, CS 1 to 4, MCS 1 to 9
UMTS Parameter		W-CDMA FDD Standard PS Datengeschwindigkeit – 384/384 kbps CS Datengeschwindigkeit – 64/64 kbps
HSDPA Parameter		3GPP rel. 5 standard Datengeschwindigkeit 3,6 Mbps /384kbps UE CAT.1 to 6,11,12 Datenkompression 3GPP TS25.212
Abmessungen	**Kunststoffgehäuse**	30x90x102 mm
	Metallgehäuse	42x86x94 mm
Temperatur-bereich	**Funktion**	-20°C bis +55°C
	Lagerung	-40°C bis +85°C
Versorgungsspannung		10 bis 30 V Gleichspannung
Verbrauch	**Ohne Sendung**	300mW
	GPRS	Bis 3,5 W
	UMTS/HSDPA	Bis 5,5 W
Antennenstecker		FME -50 OHM
Benutzerschnitt-stelle	**ETH**	Ethernet (10/100 Mbit/s)
	USB	USB 2.0 - Stecker USB-A
	Port 1	Auf Anfrage RS232/RS485/MBUS oder I/O Eingang/Ausgang

2.9. *Beschreibung der einzelnen Routerteile*

2.9.1. UMTS Modul

Für die drahtlose Kommunikation im HSDPA/UMTS/EDGE/GPRS Netz wird ein UMTS Modul angewandt. Es wird direkt auf der Platte der gedruckten Schaltungen integriert. Der ausschiebbare Halter des SIM Kartenlesers ist von der Frontplatte aus erreichbar. Der Antennenstecker ist von der Rückplatte aus erreichbar.

UMTS Modul

- Das Modul kommuniziert im UMTS Bereich 2100 MHz.
- CS Datengeschwindigkeit – 64/64 kbps.
- PS Datengeschwindigkeit – 384/384 kbps.
- Es unterstützt W-CDMA FDD (Wideband – Code Division Multiple Access Frequency Division Duplex) Standard.

2.9.2. Steuerungsmikrocomputer

Den Kern des Routers bildet ein 32-Bit Mikroprozessor mit 16 MB RAM, 4 MB FLASH EEPROM, serieller Schnittstelle RS-232 und Ethernet Schnittstelle 10/100 Mbit/s. Der Mikrocomputer wird über die USB Schnittstelle an das OEM UMTS Modul angeschlossen und steuert die HSDPA/UMTS/EDGE/GPRS Kommunikation. In Richtung zum Benutzer ist es an die Ethernet Schnittstelle angeschlossen.
Die Programmausstattung wird über das Betriebssystem uClinux aufgebaut.

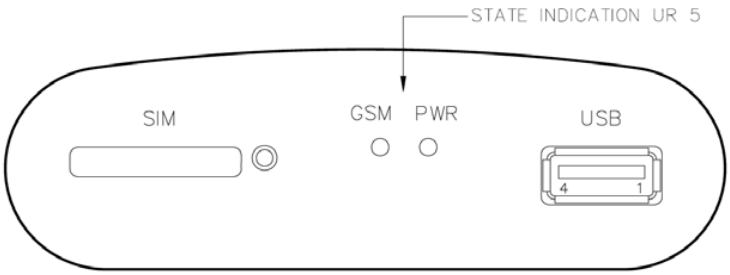
Der Router bietet die Dienste wie DHCP, NAT, GRE, IPsec Tunnel, und weitere an.

Die Routereinstellung wird im FLASH EEPROM Speicher hintergelegt. Jegliche Routerkonfiguration kann über die Webschnittstelle (HTTP) erfolgen, die mit einem Passwort abgesichert ist.

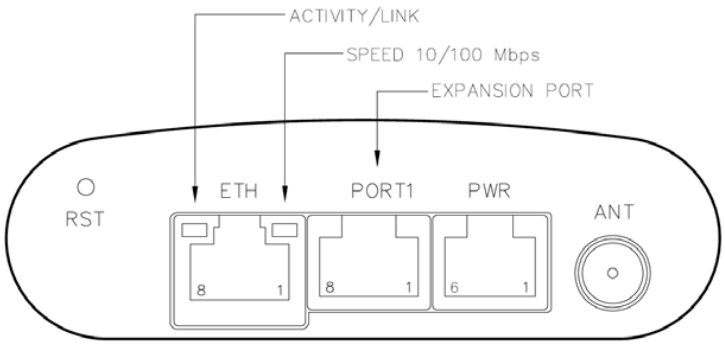
2.10. *Benutzerschnittstellen (Stecker)*

Auf der Front- und Rückplatte des Routers befinden sich:

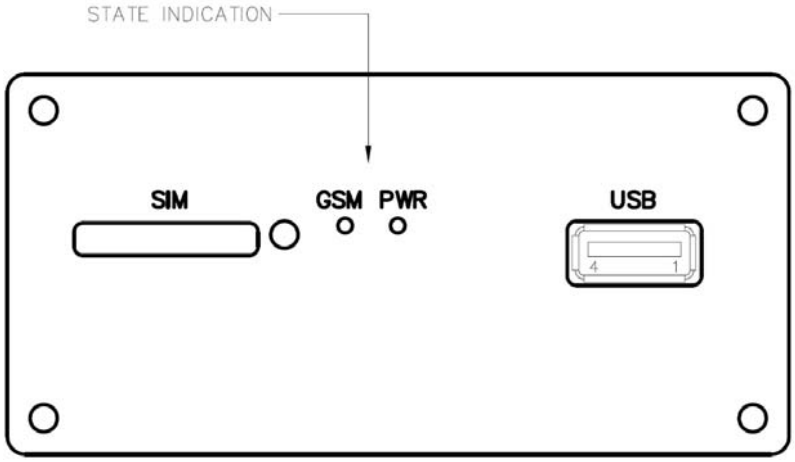
- ein Stecker RJ12 oder MRT9 (PWR) – zum Anschluss des Stromversorgungs adapters,
- ein Stecker RJ45 (ETH) – zum Anschluss an das lokale Computernetz,
- ein Stecker RJ45 (Optionsanschluss PORT1) – zum Anschluss der Geräte über RS232, RS485/422, M-BUS oder CNT,
- ein Stecker FME bzw. SMA (ANT) – zum Antennenanschluss
- ein Stecker USB-A Host (USB) – zum Anschluss der USB Geräte an den Rou ter, USB unterstützt die Geräte mit PL-2303 und FTDI USB/RS232 Umwand lern.



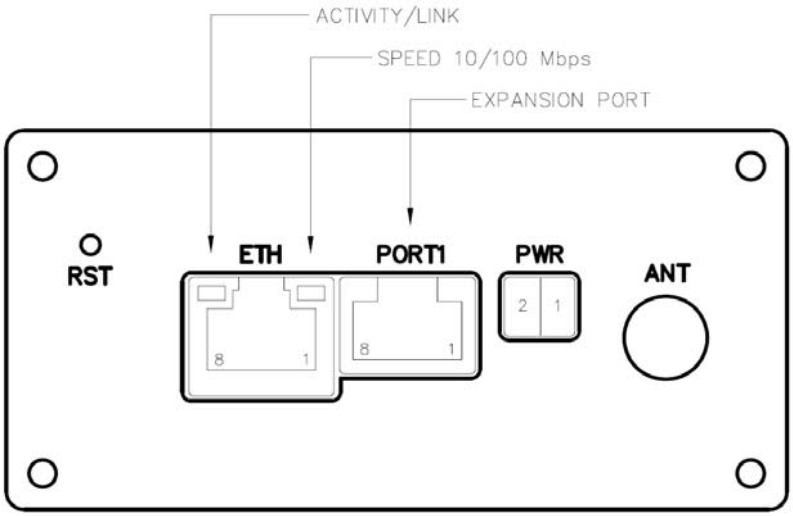
Frontplatte von UR 5



Rücklplatte von UR 5



Frontplatte von UR 5 SL



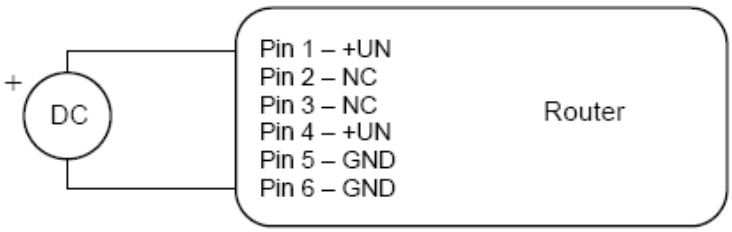
Rücklplatte von UR 5 SL

2.10.1. Belegung des PWR Stromversorgungssteckers

• Gerätebuchse RJ12

Stift-nummer	Signalbe-zeichnung	Beschreibung
1	+UN	Pluspol der Versorgungsgleichspannung (10 bis 30 V)
2	NC	Signal nicht belegt
3	NC	Signal nicht belegt
4	+UN	Pluspol der Versorgungsgleichspannung (10 bis 30 V)
5	GND	Minuspol der Versorgungsgleichspannung
6	GND	Minuspol der Versorgungsgleichspannung

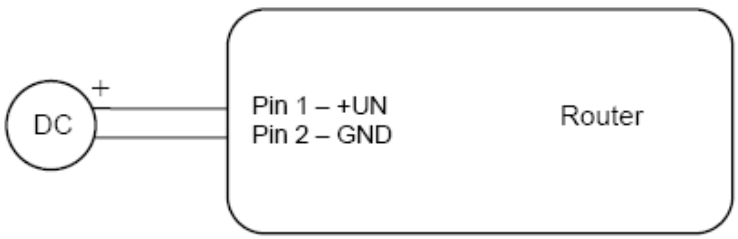
Belegungsbeispiel:



• Gerätebuchse MRT9.

Stift-nummer	Signalbe-zeichnung	Beschreibung
1	+UN	Pluspol der Versorgungsgleichspannung (10 bis 30 V)
2	GND	Minuspol der Versorgungsgleichspannung

Belegungsbeispiel:



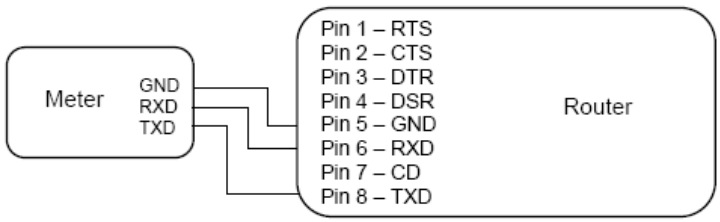
Auf dem Versorgungsnetzteil ist +UN mit roter Hülse gekennzeichnet.

2.10.2. Belegung des Steckers PORT1 – RS232

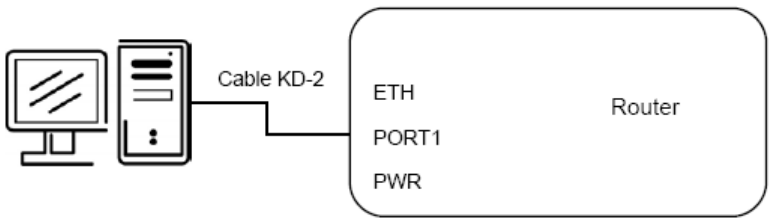
Gerätebuchse RJ45 (RS232 – DCE – Data Communication Equipment)

Stift-nummer	Signalbe-zeichnung	Beschribung	Datenflussrichtung
1	RTS	Request to Send	Eingang
2	CTS	Clear To Send	Ausgang
3	DTR	Data Terminal Ready	Eingang
4	DSR	Data Set Ready – auf +4 V über Widerstand R 330 Ohm angeschlossen	Ausgang
5	GND	GROUND – signal ground	
6	RXD	Receive Data	Ausgang
7	CD	Carrier Detect	Ausgang
8	TXD	Transmit Data	Eingang

Beispiel für den Anschluss des Messgerätes an den Router:

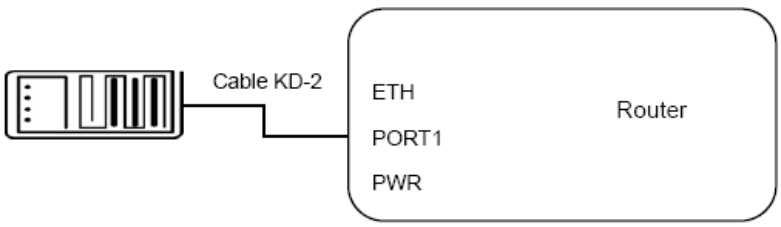


Beispiel vom Anschluss des Routers zum PC:



• Das Kabel KD2 wird an den PC an den seriellen Anschluss (z. B. COM1) angeschlossen

Beispiel für den Anschluss des Routers an ein Gerät mit vollwertiger Schnittstelle:



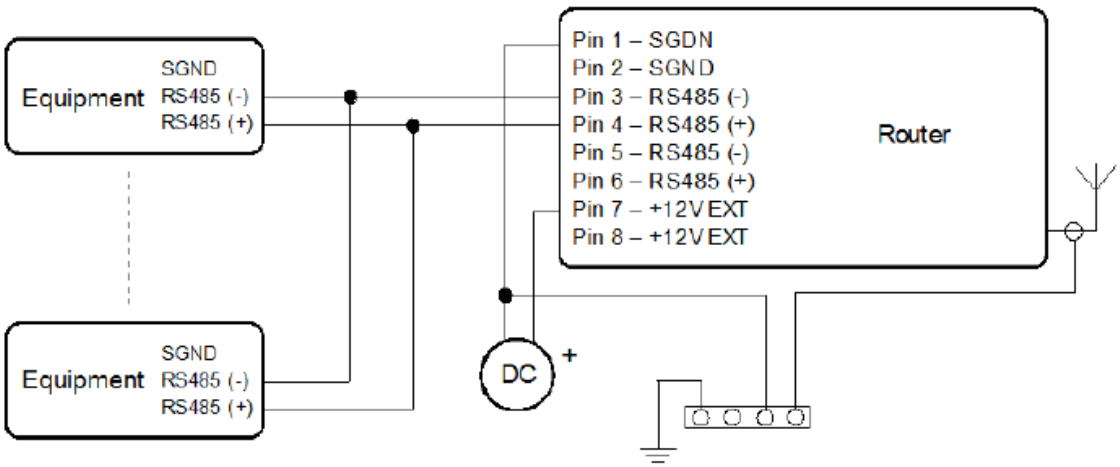
2.10.3. Belegung des Steckers PORT1 - RS485

Gerätebuchse RJ45

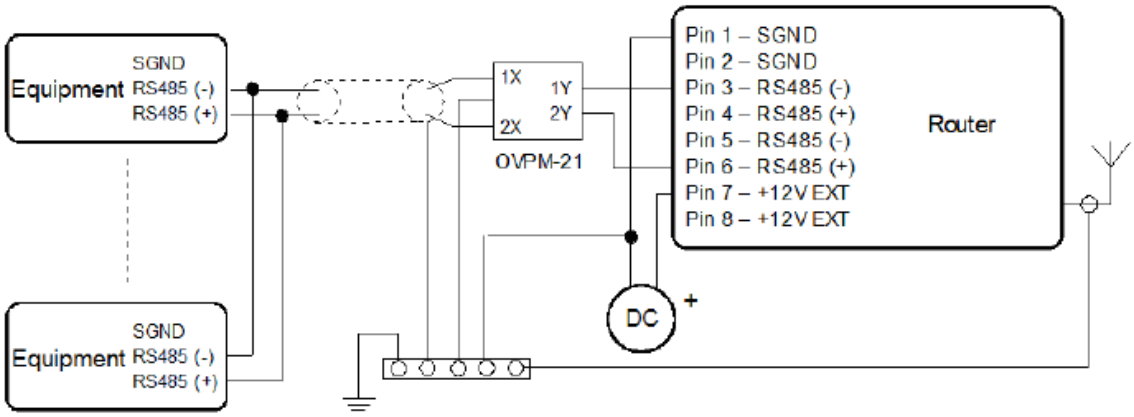
Stift-nummer	Signalbe-zeichnung	Beschreibung	Datenflussrichtung
1	SGND	Signalerde und Erde der Stromversorgung	
2	SGND	Signalerde und Erde der Stromversorgung	
3	TxRx-	RS485 B (-)	Eingang / Ausgang
4	TxRx+	RS485 A (+)	Eingang / Ausgang
5	TxRx-	RS485 B (-)	Eingang / Ausgang
6	TxRx+	RS485 A (+)	Eingang / Ausgang
7	+12 V EXT	Externe Stromversorgung	
8	+12 V EXT	Externe Stromversorgung	

Vorsicht! Die Stromversorgung wird am Erweiterungsanschluss RS485 mit Brückenverbinder gewählt, siehe Kap. 2.11.
Im Bedarfsfall der galvanischen Abtrennung muss der Umwandler aus externer Stromversorgung gespeist werden.

Beispiel für den Anschluss des Messgeräts an den Router bei einer Länge des Datenkabels <10 m:



Beispiel für den Anschluss des Messgeräts an den Router bei einer Länge des Datenkabels >10 m:



Bei einer Länge der Datenleitung RS485 >10 m ist es notwendig, auf der Routerseite Schutzanlagen gegen Überspannung zu verwenden!

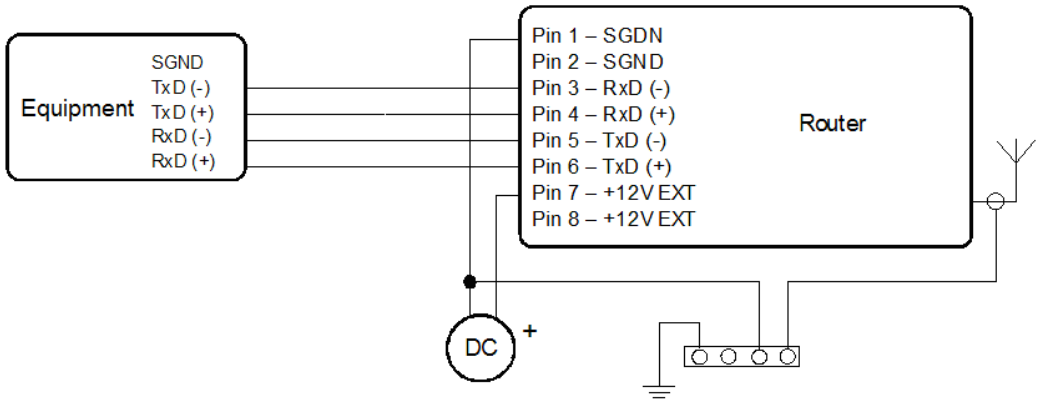
2.10.4. Belegung des Steckers PORT1 – RS422

Gerätebuchse RJ45

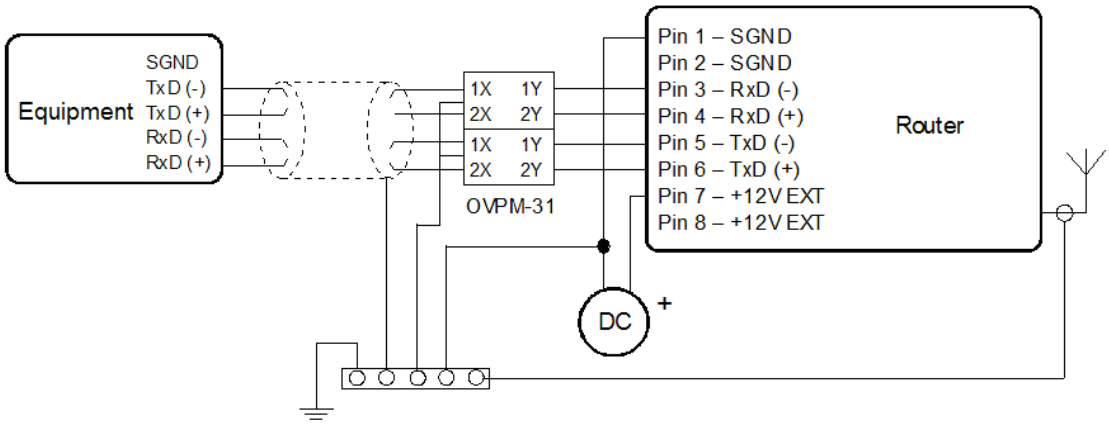
Stift-nummer	Signalbe-zeichnung	Beschreibung	Datenflussrichtung
1	SGND	Signalerde und Erde der Stromversorgung	
2	SGND	Signalerde und Erde der Stromversorgung	
3	RxD-	Receive Data (-)	Ausgang
4	RxD+	Receive Data (+)	Ausgang
5	TxD-	Transmit Data (-)	Eingang
6	TxD+	Transmit Data (+)	Eingang
7	+12V EXT	Externe Stromversorgung	
8	+12V EXT	Externe Stromversorgung	

Vorsicht! Die Stromversorgung wird am Erweiterungsanschluss RS422 mit dem Brückenverbinder gewählt, siehe Kap. 2.11.
Im Bedarfsfall der galvanischen Abtrennung muss der Umwandler aus externer Stromversorgung gespeist werden.

Beispiel für den Anschluss des Messgeräts an den Router bei einer Länge des Datenkabels <10 m:



Beispiel für den Anschluss des Messgeräts an den Router bei einer Länge des Datenkabels >10 m:



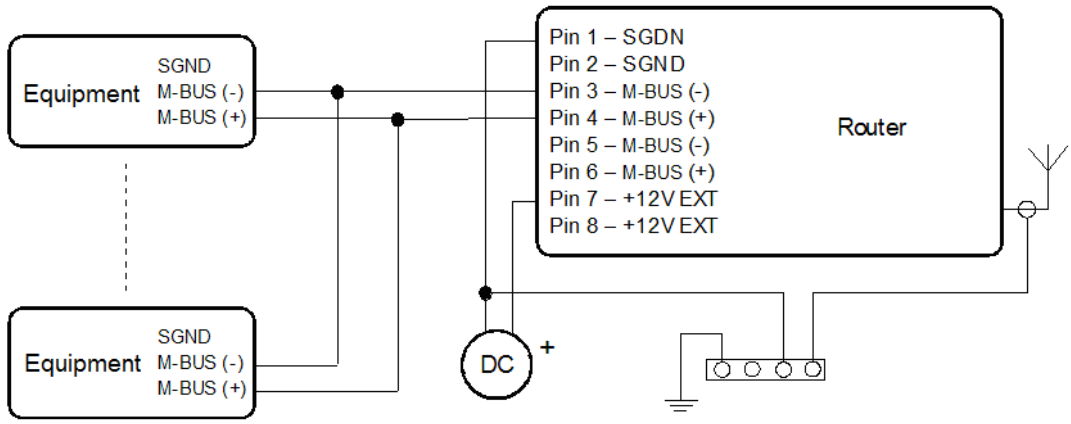
Bei der Länge der Datenleitung RS422 >10 m ist es notwendig, auf der Routerseite Schutzanlagen gegen Überspannung zu verwenden!

2.10.5. Belegung des Steckers PORT1 - M-BUS

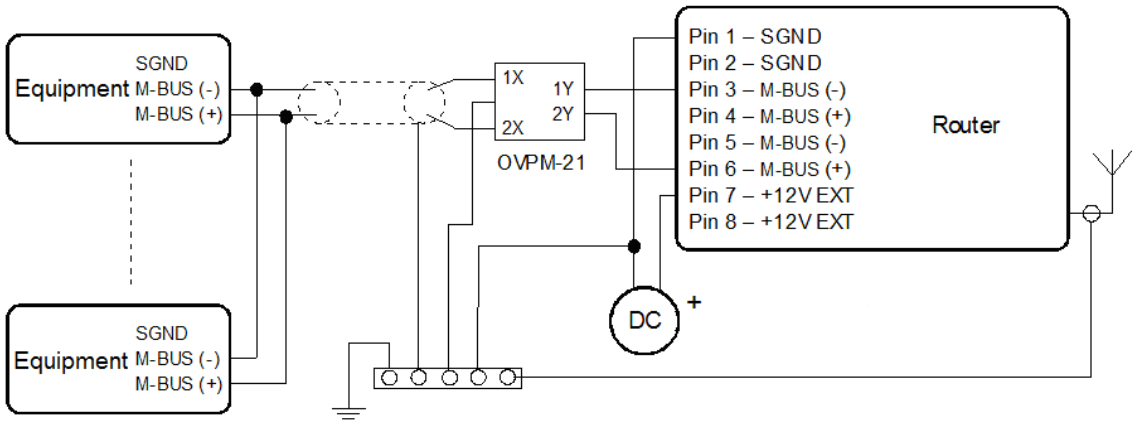
Gerätebuchse RJ45

Stift-nummer	Signalbe-zeichnung	Beschreibung	Datenflussrichtung
1	GND	Signalerde und Erde der Stromversorgung	
2	GND	Signalerde und Erde der Stromversorgung	
3	TxRx-	MBUS B (-)	Eingang / Ausgang
4	TxRx+	MBUS A (+)	Eingang / Ausgang
5	TxRx-	MBUS B (-)	Eingang / Ausgang
6	TxRx+	MBUS A (+)	Eingang / Ausgang
7	+12 V EXT	Externe Stromversorgung	
8	+12 V EXT	Externe Stromversorgung	

Vorsicht! Die externe Stromversorgung dient dem Erweiterungsanschluss MBUS!
Im Bedarfsfall der galvanischen Abtrennung muss der Umwandler aus externer Stromversorgung gespeist werden.
Beispiel für den Anschluss des Messgeräts an den Router bei einer Länge des Datenkabels <10 m:



Beispiel für den Anschluss des Messgeräts an den Router bei einer Länge des Datenkabels >10 m:



Bei Länge der Datenleitung M-BUS >10 m ist es notwendig, auf der Routerseite Schutzanlagen gegen Überspannung zu verwenden!

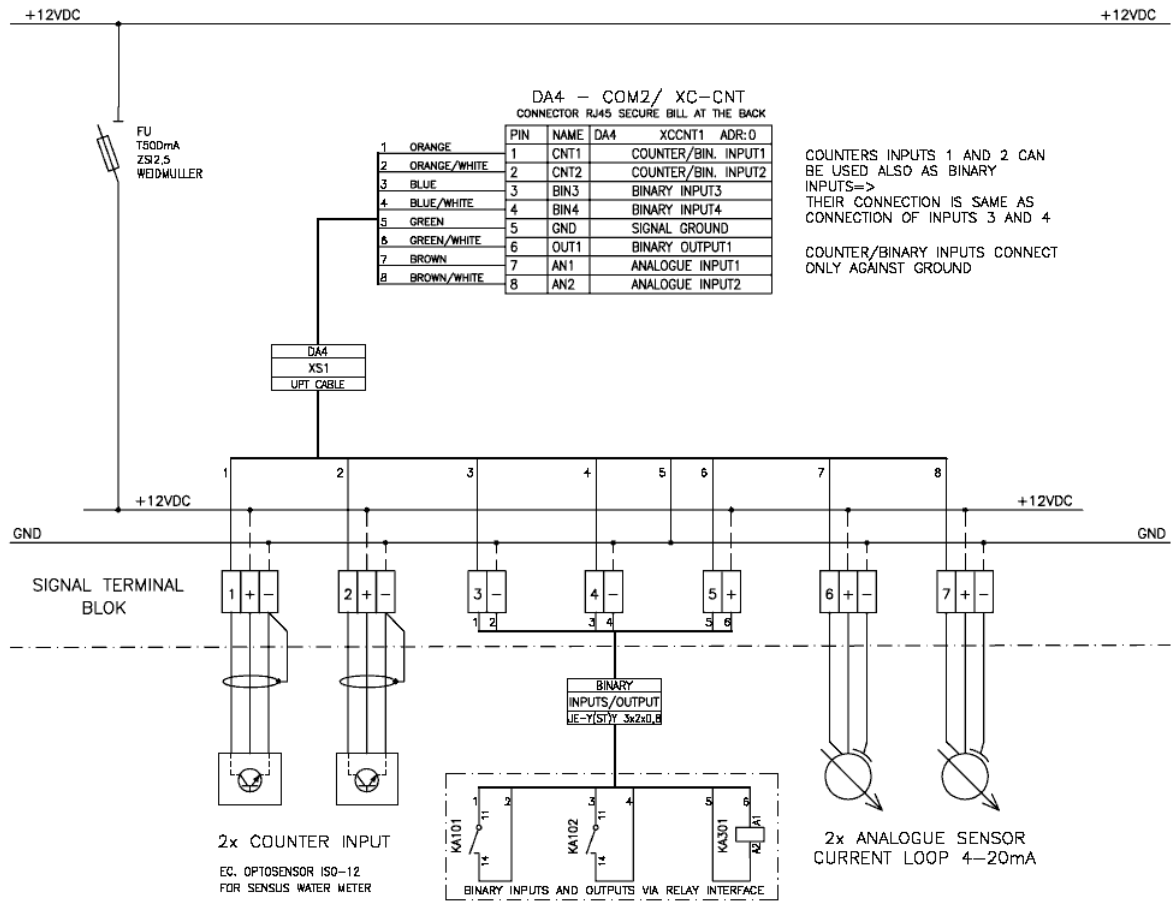
2.10.6. Belegung des Steckers PORT1 - CNT

Gerätebuchse RJ45

Stift-nummer	Signalbe-zeichnung	Beschreibung	Datenflussrichtung
1	BIN1/CNT1	Binäreingang / Zahleingang	Eingang
2	BIN2/CNT2	Binäreingang / Zahleingang	Eingang
3	BIN3	Binäreingang	Eingang
4	BIN4	Binäreingang	Eingang
5	GND	Signalerde	
6	OUT1	Binärausgang (offener Kollektor)	Ausgang
7	AN1	Analogeingang	Eingang
8	AN2	Analogeingang	Eingang

Die Benutzerschnittstelle ist zum Abgreifen und zur Bearbeitung von analogen und binären Signalen sowie zur Steuerung (Einstellung) des Binärsignals vorgesehen. Es stehen 2 Zahl- und 2 Binäreingänge oder 4 Binäreingänge, 2 Analogeingänge und 1 Binärausgang zur Verfügung. Die Einstellung der Binär- und Zahleingänge erfolgt mit der Firmware, in der die einzelnen Eingänge und Ausgänge definiert werden.

Typischer Anschluss von Messkreisen des Routers:



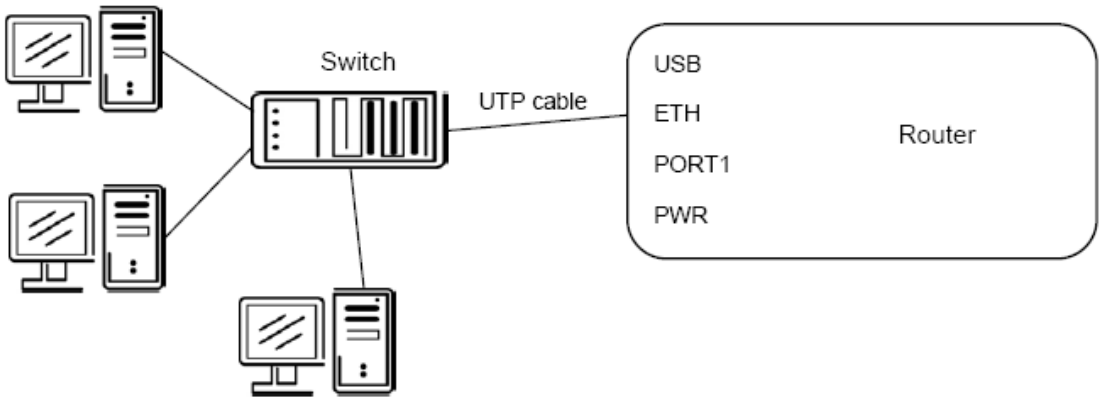
2.10.7. Belegung des Steckers ETH

Gerätebuchse RJ45

Stift-nummer	Signalbe-zeichnung	Beschreibung	Datenflussrichtung
1	TXD+	Transmit Data – Pluspol	Eingang / Ausgang
2	TXD-	Transmit Data – Minuspol	Eingang / Ausgang
3	RXD+	Receive Data – Pluspol	Eingang / Ausgang
4	—-	—-	
5	—-	—-	
6	RXD-	Receive Data – Minuspol	Eingang / Ausgang
7	—-	—-	
8	—-	—-	

Vorsicht! Der Anschluss ETH ist mit POE (Power Over Ethernet) nicht kompatibel!

Belegungsbeispiel beim ETH Router:

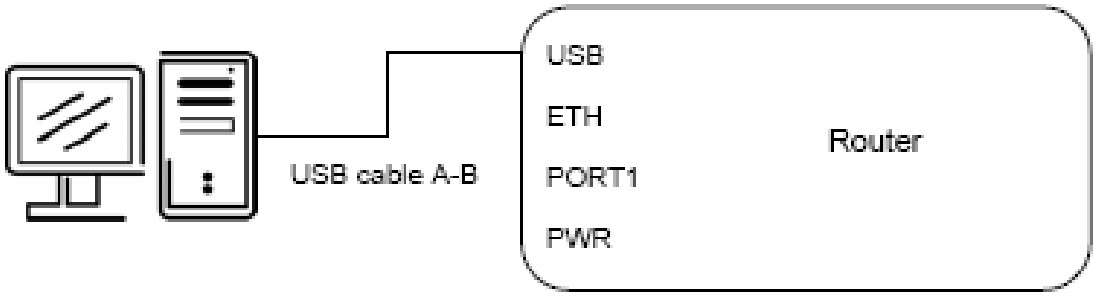


2.10.8. Connection of the Connector USB

Panel socket USB-A.

Stift-nummer	Signalbe-zeichnung	Beschreibung	Datenflussrichtung
1	VCC	Pluspol der Versorgungsgleichspannung 5 V	
2	USB data-	Datensignal USB - Minuspol	Eingang / Ausgang
3	USB data+	Datensignal USB - Pluspol	Eingang / Ausgang
4	GND	Minuspol der Versorgungsgleichspannung	

Belegungsbeispiel beim USB Router:



2.11. *Technische Spezifikationen des Optionsanschlusses PORT1:*

• Erweiterunganschluss RS232

Expansion port RS232		
Stromversorgung	Intern	....
Betriebsbedingungen	Betriebstemperatur	-20 .. +55 °C
	Lagerungstemperatur	-20 .. +85 °C
Entspricht den Normen	Emissionen	EN 55022/B
	Verträglichkeit	ETS 300 342
	Sicherheit	EN 60950
RS232 Spezifikationen (EN 1434)	Max. Belastung	15 mA
	Max. Übertragungsgeschwindigkeit	230400 bps
	Max. Überspannung	±30 V
	Max. Kabellänge (300 Bd, 200nF/km)	20 m

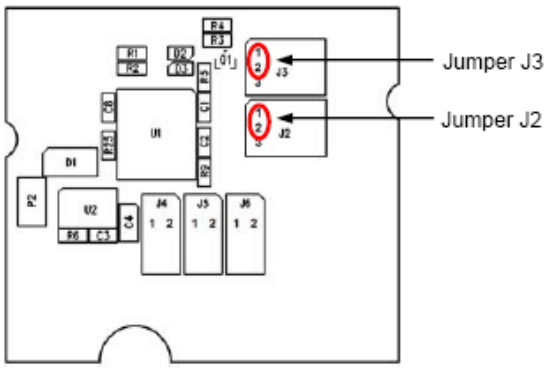
• Erweiterungsanschluss RS485-RS422

Expansion port RS485-RS422		RS485	RS422
Stromversorgung	Extern	+10 .. +30 V	
	Intern	....	
	Leistungsaufnahme	Max. 1 W	
	Verbrauch	Max. 4 mA	
Betriebsbedingungen	Betriebstemperatur	-20 .. +55 °C	
	Lagerungstemperatur	-20 .. +85 °C	
Entspricht den Normen	Emissionen	EN 55022/B	
	Verträglichkeit	ETS 300 342	
	Sicherheit	EN 60950	
RS485 Spezifikationen (EN 1434)	Max. Geräteanzahl (je 1,5 mA)	256	
	Max. Übertragungsgeschwindigkeit	38400 bps	
	Kurzschlussfestigkeit	Permanent	
	Max. Kabellänge (300 Bd, 200nF/km)	1200 m	

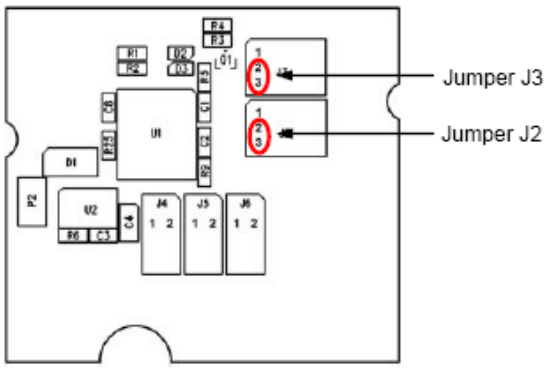
Externe oder interne Stromversorgung des Moduls Expansion Port RS485/RS422 kann durch den Anschluss der Brückenverbinder J2 und J3 an dieses Modul gewählt werden. Ist die externe Stromversorgung des Moduls erwünscht, müssen die Stifte 2–3 mit dem Brückenverbinder J2 und J3 verbunden werden. Die Interne Stromversorgung wird mit der Verbindung der Stifte 1–2 mit dem Brückenverbinder J2 und J3 gewählt.

Das Verhalten der Schnittstelle RS485 oder RS422 kann durch den Anschluss der Brückenverbinder J4, J5 und J6 an dieses Modul gewählt werden. Ist das Verhalten der Schnittstelle RS485 erwünscht, müssen die Brückenverbinder J4 und J5 geschlossen und der Brückenverbinder J6 geöffnet werden. Ist das Verhalten der Schnittstelle RS422 erwünscht, müssen die Brückenverbinder J4 und J5 geöffnet und der Brückenverbinder J6 geschlossen werden.

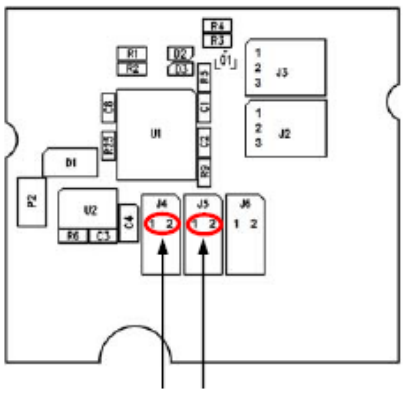
Die örtliche Verteilung der Brückenverbinder ist auf dem unteren Bild (Modul Expansion Port RS485/RS422 von der Oberseite TOP) zu sehen. Die interne Stromversorgung ist nur dann zu empfehlen, wenn es nicht möglich ist eine externe Stromversorgung sicherzustellen. Ist die interne Stromversorgung gewählt, ist der Umwandler RS485/RS422 galvanisch getrennt.



The jumper circuitry for internal supply



The jumper circuitry for external supply



The jumper circuitry for RS485

The jumper circuitry for RS422

• Erweiterunganschluss MBUS

Expansion port MBUS		
Stromversorgung	Versorgungsspannung	+10 .. +30 V
	Leistungsaufnahme	Max. 4 W
Betriebsbedingungen	Betriebstemperatur	-20 .. +55 °C
	Lagerungstemperatur	-20 .. +85 °C
Entspricht den Normen	Emissionen	EN 55022/B
	Verträglichkeit	ETS 300 342
	Sicherheit	EN 60950
M-Bus specifications (EN 1434)	Max. Geräteanzahl (je 1,5 mA)	30
	Max. Leistungsaufnahme beim Bus im Arbeitsbetrieb	60 mA
	Erfassung der Überlastung	100 mA
	Kurzschlussfestigkeit	Permanent
	Busspannung Zeichen	36 .. 43 V
	Busspannung Leerzeichen	24 .. 31 V
	Max. Kabellänge (300Bd, 200nF/km)	1000 m

- Expansion port CNT

Expansion port CNT		
Stromversorgung	Intern	….
	Passive Betriebsbereitschaft	100 µA (counter is functional)
	Betrieb	2 mA
Betriebsbedingungen	Betriebstemperatur	-20 .. +55 °C
	Lagerungstemperatur	-20 .. +85 °C
Entspricht den Normen	Emissionen	EN 55022/B
	Verträglichkeit	ETS 300 342
	Sicherheit	EN 60950
Eingänge / Ausgänge	2x Zählereingänge	Max. 100 Hz, ratio max. 1:10
	2x Analogeingänge	0 .. 20 mA, Rin 100 Ohms
	2x Binäreingänge	Potentialfreier Kontakt
	1x Ausgang (offener Kollektor)	100 mA
Sonstiges	Überspannungsfestigkeit	dauerhaft
	Modus passiver Betriebsbereitschaft	gesteuert

2.12. *Anzeige des Routerzustandes*

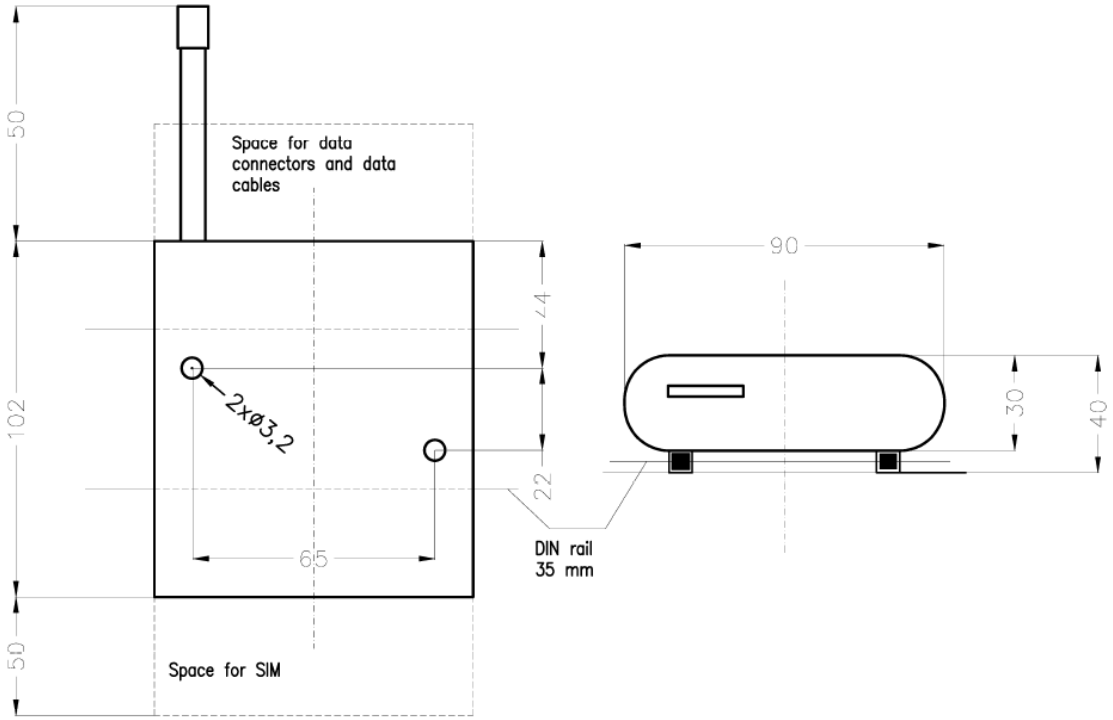
Auf der Front- und Rückplatte des Routers befinden sich insgesamt vier Kontrollleuchten (LED), die über den Routerstand informieren.

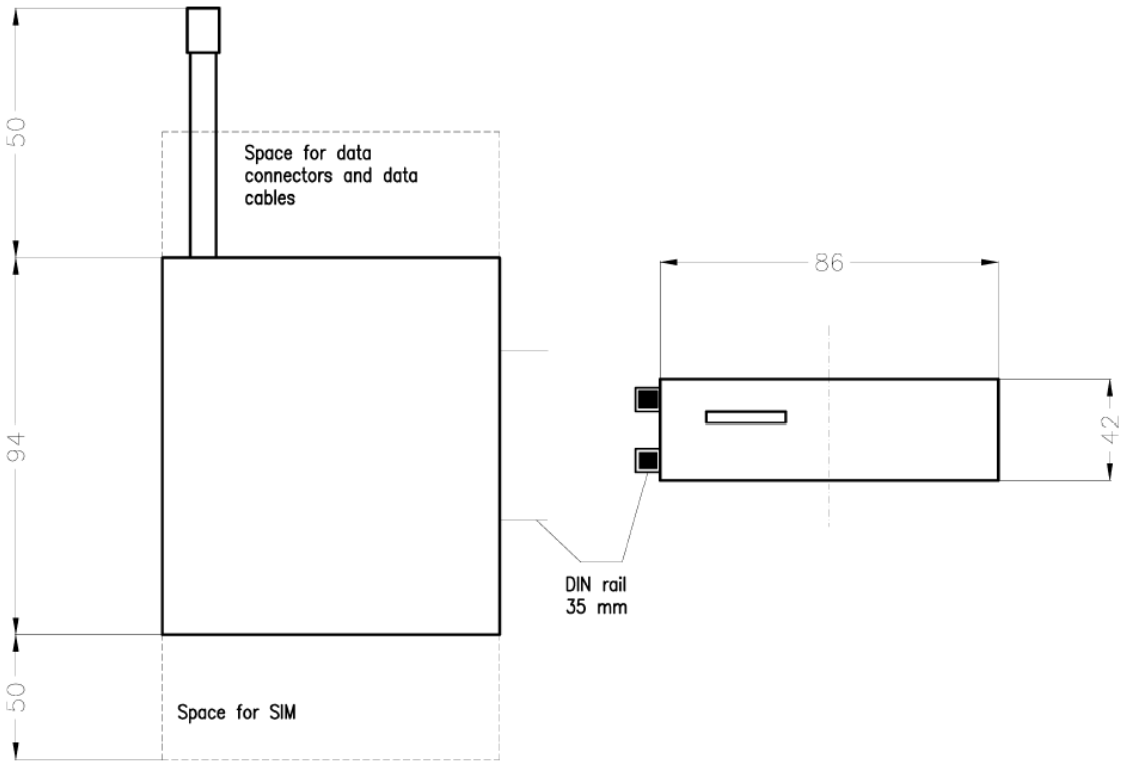
Platte	Farbe	Beschreibung	Bedeutung
Front platte	Grün	PWR	Sie blinkt 1:9 ……..... die Verbindung wurde aufgebaut Sie blinkt 9:1 ……..... die Verbindung wird aufgebaut Sie leuchtet ununterbrochen …. das Einschalten des Routers läuft
Front platte	Rot	GSM	Sie blinkt ……..... die Kommunikation läuft
Rück platte	Grün	-	Sie leuchtet ununterbrochen …..die Geschwindigkeit von 100 Mbit/s in Ethernet gewählt Sie leuchtet nicht …..die Geschwindigkeit von 10 Mbit/s in Ethernet gewählt
Rück platte	Grün	-	Sie leuchtet ununerbrochen ….. das Netzkabel ist angeschlossen Sie blinkt ……..... die Datenübertragung läuft Sie blinkt ……..... die Datenübertragung läuft

2.13. *Inbetriebsetzung*

Bevor Sie den Router in Betrieb setzen, ist es notwendig, alle für den Lauf Ihrer Anwendungen erforderlichen Bestandteile einzuschalten und darüber hinaus muss die SIM Karte eingelegt werden (der Router ist dabei ausgeschaltet).
Der Router wird durch den Anschluss des Versorgungsnetzteils an den Router in Betrieb gesetzt. In der Ausgangseinstellung fängt der Router an, sich in das voreingestellte APN automatisch anzumelden. Das Routerverhalten kann mittels der im Folgekapitel beschriebenen Webschnittstelle geändert werden.

2.14. *Mechanische und Einbauabmessungen sowie Empfehlungen zur Montage*



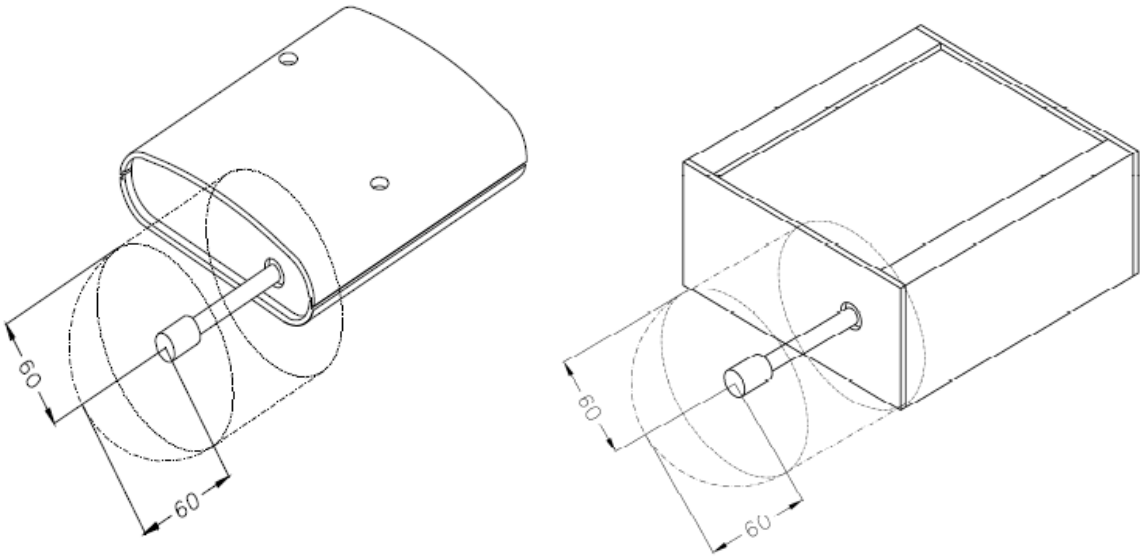


Bei den meisten Anwendungen mit dem im Schaltschrank eingebauten Modem ist es möglich, zwei Umgebungsarten zu unterscheiden:

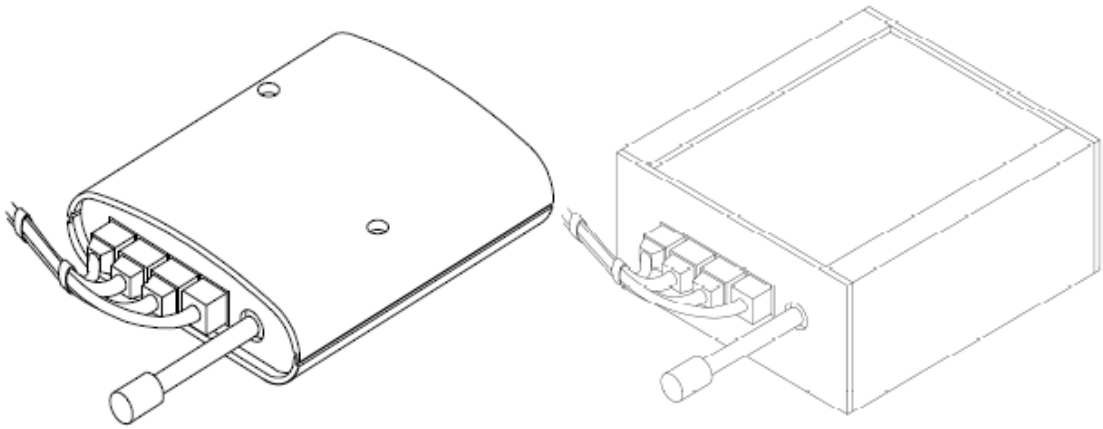
- nicht öffentliche und industrielle Umgebung in Niederspannung mit großer Störung,
- öffentliche Stellen in Niederspannung ohne große Störung

Für beide von diesen Umgebungen ist es möglich, die Router in den Schaltschrank einzubauen, anschließend ist es nicht notwendig, Beständigkeits- oder Emissionsprüfungen im Zusammenhang mit der EMV im Sinne der Norm EN 60439-1 ed.2 durchzuführen.
Zur Einhaltung der Norm EN 60439-1 ed.2 ist es notwendig, folgende Montage des Routers in den Schaltschrank durchzuführen:

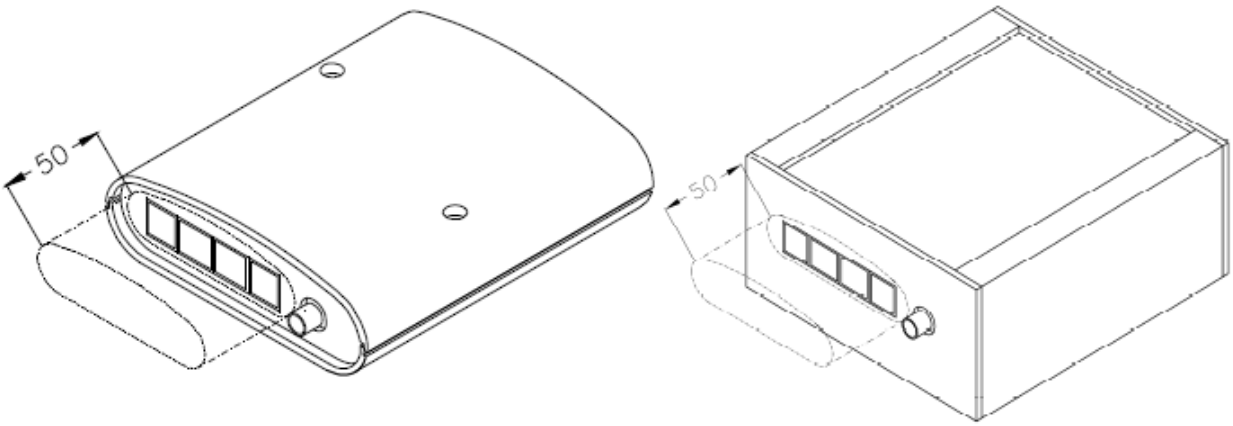
- es wird empfohlen, rund um die Antenne einen Abstand von 6 cm von Kabeln und Metallflächen auf jeder Seite laut dem folgenden Bild zur Vermeidung einer Störungen einzuhalten, bei der Verwendung von externen Antenne außerhalb des Schaltschrankes ist es notwendig, die geeigneten Schutzanlagen gegen Überspannung (Blitzableiter) einzusetzen,
- bei Montage des Routers auf das Stahlblech wird empfohlen eine externe An tenne zu verwenden,



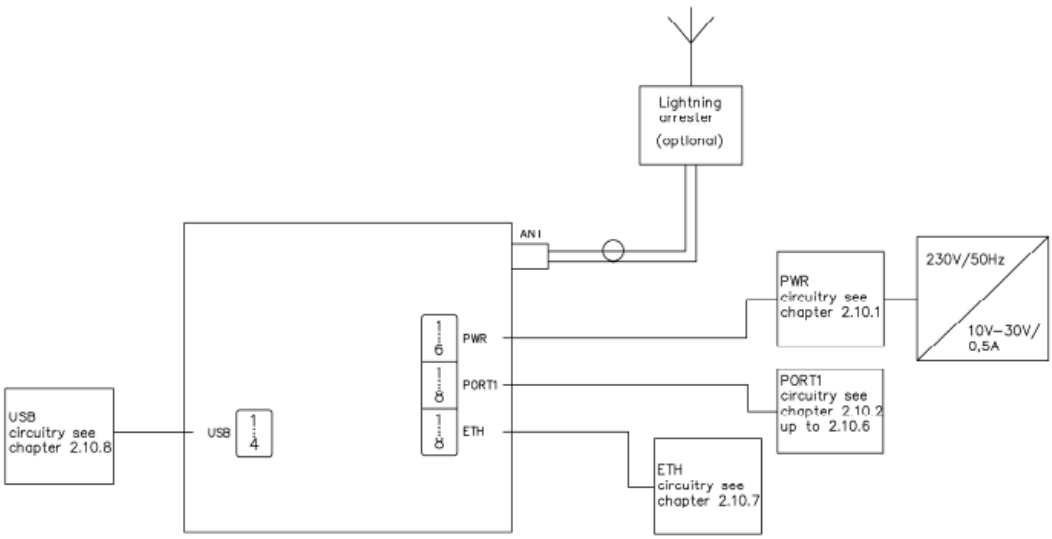
- es wird empfohlen, die einzelnen Kabel in ein Bündel (siehe Bild weiter unten) einzubinden. Für die auf diese Weise geführten Kabel gelten folgende Begren zungen:
  - die Bündellänge (Kombination der Stromversorgungs- und Datenka bel) kann maximal 1,5 m betragen, überschreitet die Länge der Da tenkabel 1,5 m oder im Falle, dass die Datenkabel außerhalb des Schaltschrankes geführt werden, wird empfohlen, eine geeigneten Schutzanlagen gegen Überspannung (Blitzableiter) zu verwenden,
  - zusammen mit den Datenkabeln dürfen nicht die Kabel, die Netzspannung ~ 230 V/50 Hz übertragen, geführt werden,
  - die Signale zu den Sensoren müssen mit den verdrillten Paaren ge führt werden,



- vor den einzelnen Steckverbindern muss ein gewisser Abstand zur Handhabung von Kabeln beim etwaigen Anschließen und Abtrennen der einzelnen Kabel be stehen bleiben,



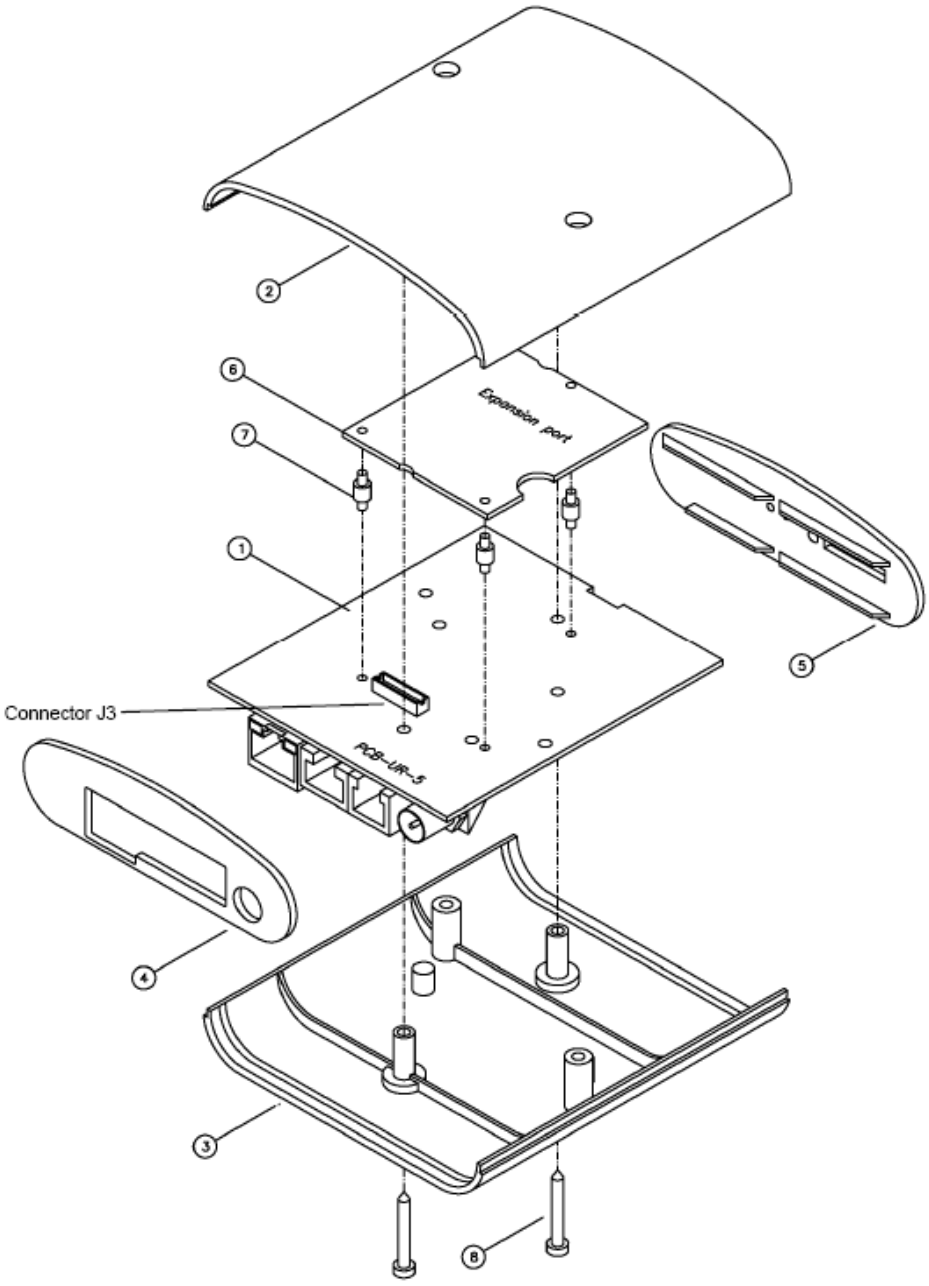
- für die richtige Funktion des Routers wird empfohlen, im Schaltschrank die Erdungsklemmleiste zur Erdung des Versorgungsnetzteils für das Modem, das Datenkabel und die Antenne zu verwenden,
- der Anschluss des Routers ist aus dem folgenden Bild ersichtlich:



3. Einsatz des Erweiterungsanschlusses

3.1. *Einsatz des Erweiterungsanschlusses des Routers UR 5*

Vorsicht! Der Erweiterungsanschluss PORT1 wird angeschlossen, während der UR 5 Router abgeschaltet ist.
Nach dem Abschrauben von zwei Schrauben (Pos. 8) am unteren Gehäuseteil (Pos. 3) und nach dem Abnehmen des oberen Gehäuseteils (Pos. 2) wird der Erweiterungsanschluss PORT1 (Pos. 6) in den Steckverbinder J3 (siehe Bild unten) der Grundplatte des Routers UR- 5 (Pos. 1) von der TOP Seite angeschlossen. Der Erweiterungsanschluss wird zur Grundplatte des Routers mit 3 Stück Abstand haltender Säulen (Pos. 7) befestigt. Nach dem Aufsetzen des Anschlusses wird das Gehäuse mit den Schrauben (Pos. 8) wieder Zu sammengeschraubt.



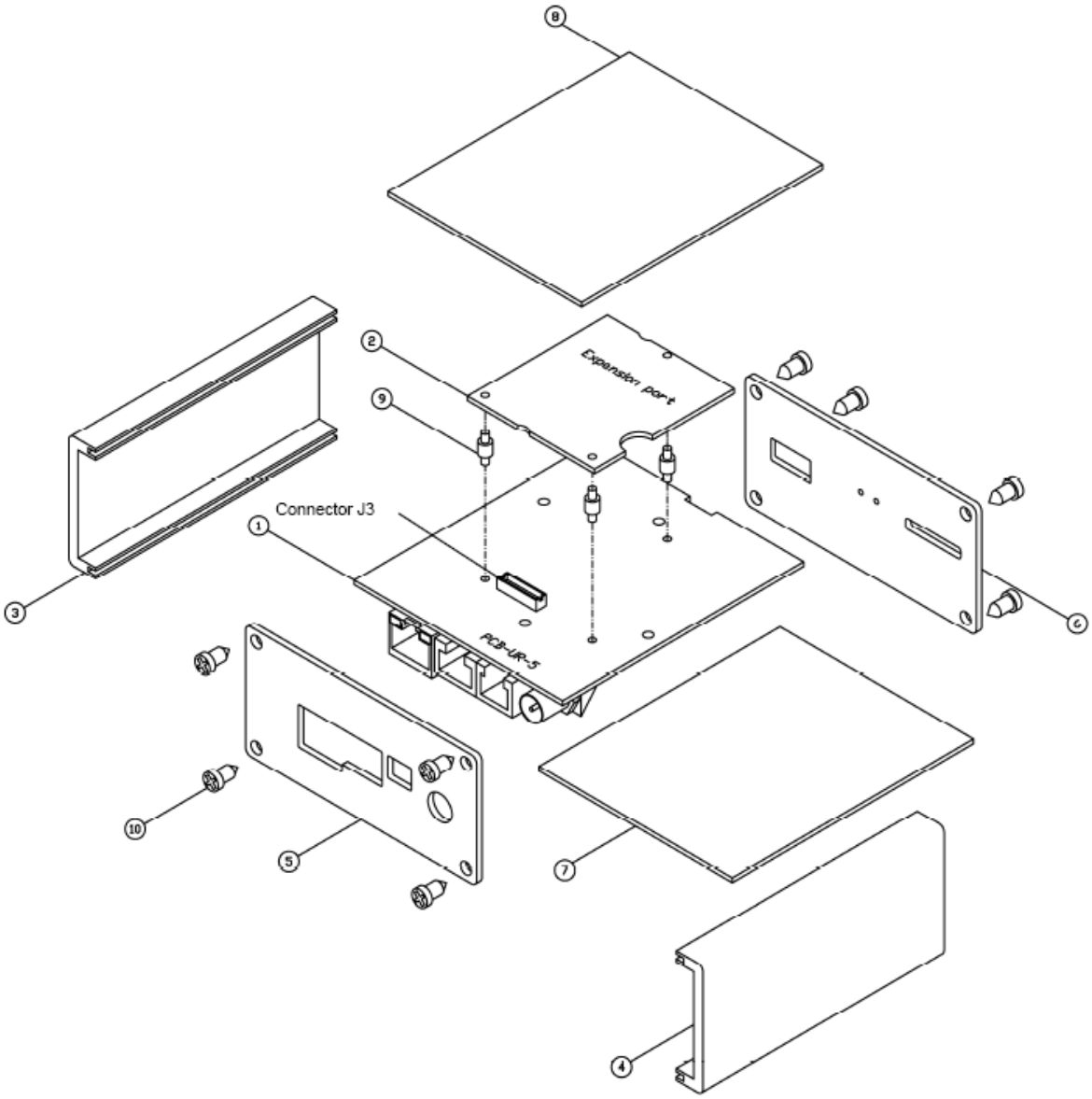
Liste und Beschreibung der Teile

Teil	Beschreibung	Anzahl
1	Grundplatte des UMTS Routers	1
2	Oberer Gehäuseteil	1
3	Unterer Gehäuseteil	1
4	Hinterer Frontteil	1
5	Vorderer Frontteil	1
6	Erweiterungsanschluss PORT1	1
7	Abstand haltende Säule zur Befestigung des Erweiterungs-anschlusses PORT1 zur Grundplatte	3
8	Schrauben zur Fertigstellung des Gehäuses	2

3.2. *Einsatz des Erweiterungsanschlusses des Routers UR 5 SL*

Vorsicht! Der Erweierungsanschluss PORT1 wird angeschlossen, während der Router UR 5 SL abgeschaltet ist.

Nach dem Abschrauben von vier Schrauben (Pos. 10) am hinteren Frontteil des Gehäuses (Pos. 5) und nach dem Abnehmen ist es möglich, die Platte ER-75i (Pos. 1) herauszuschieben. Der Erweiterungsanschluss (Pos. 2) wird in den Steckverbinder J3 (unteres Bild) der Grundplatte des Routers B-ER-75i (Pos. 1) von der TOP Seite angeschlossen. Der Erweiterungsanschluss wird zur Grundplatte des Routers mit 3 Stück Abstand haltender Säulen (Pos. 9) befestigt. Nach dem Aufsetzen des Anschlusses wird das Gehäuse mit Schrauben (Pos. 10) wieder zusammengeschraubt.



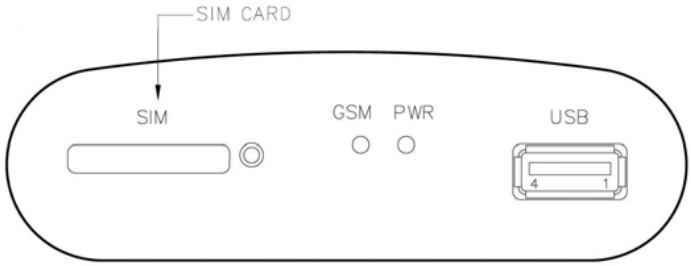
Liste und Beschreibung der Teile

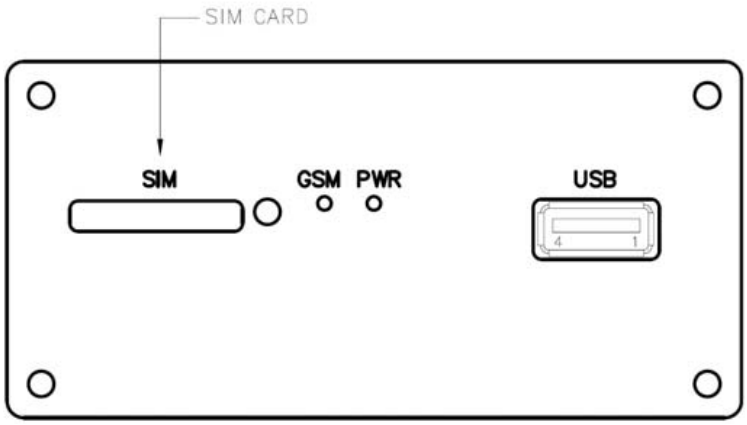
Teil	Beschreibung	Anzahl
1	Grundplatte des UMTS Routers	1
2	Erweiterungsanschluss PORT1	1
3	Linke Seitenwand des Routers	1
4	Rechte Seitenwand des Routers	1
5	Hinterer Frontteil des Routers	1
6	Vorderer Frontteil des Routers	1
7	Unterer Gehäuseteil des Routers	1
8	Oberer Gehäuseteil des Routers	1
9	Abstand haltende Säule zur Befestigung des Erweiterungsanschlusses zur Grundplatte	3
10	Schraube zur Fertigstellung des Gehäuses	8

4. Austausch der SIM Karten

Vorsicht! Die SIM Karte wird ausgetauscht, während der Router ausgeschaltet ist.

Austausch der SIM Karte auf der vorderen Frontplatte:
Vergewissern Sie sich, dass Router nicht unter Spannung steht. Lassen Sie den Leserhalter durch die Betätigung der kleinen gelben Taste neben dem Leser herausfahren. Legen Sie die SIM Karte in den Leserhalter ein und lassen Sie diesen in den Leser hineinfahren.

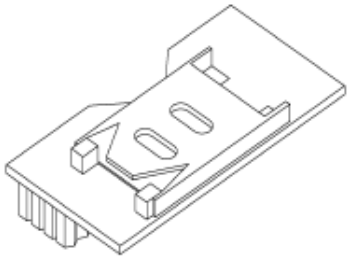




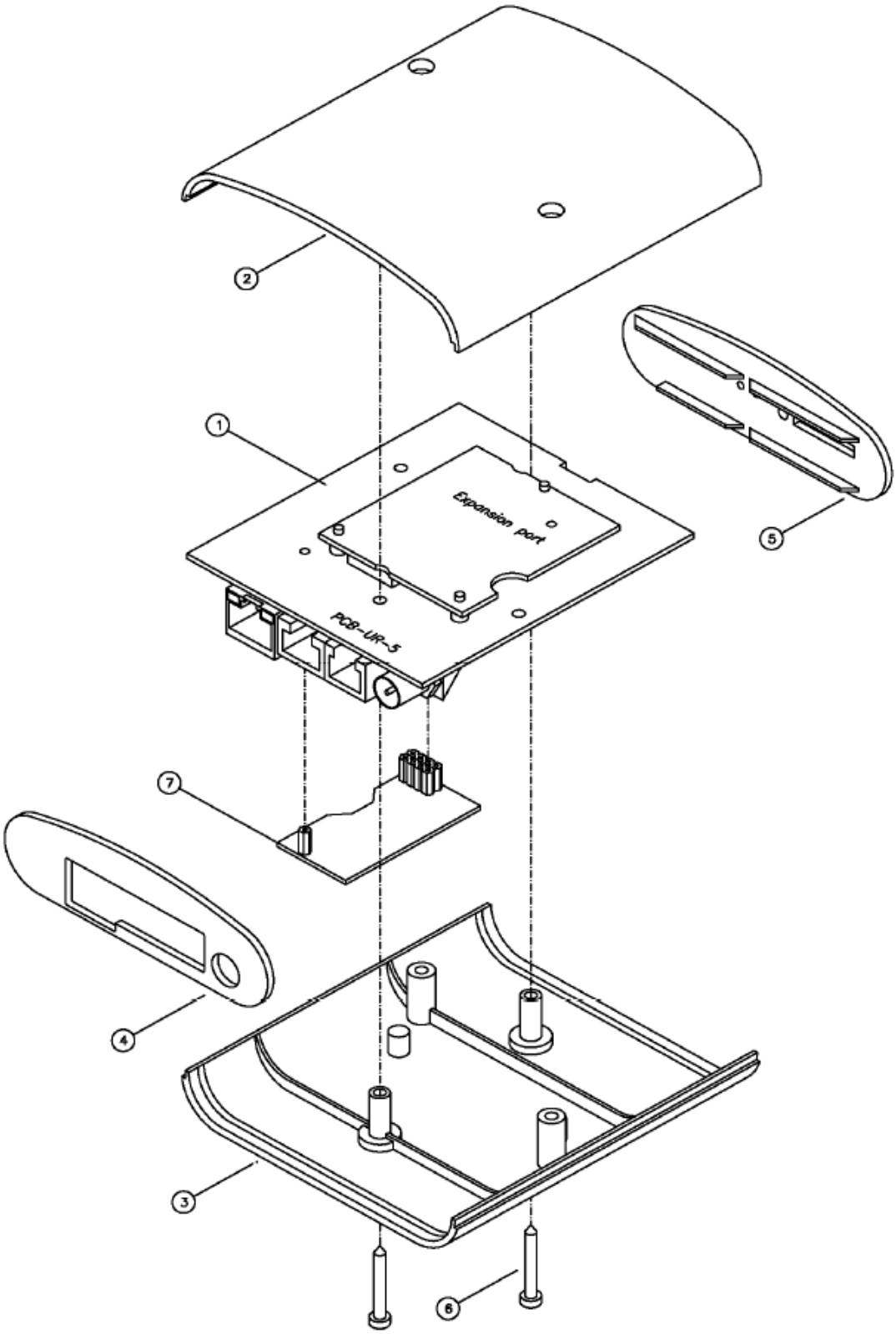
4.1. *Austausch der zweiten SIM Karte beim Router UR 5*

Nach dem Abschrauben von zwei Schrauben (Pos. 6) am unteren Gehäuseteil (Pos. 3) und nach dem Abnehmen des oberen Gehäuseteils (Pos. 2) ist es möglich, die SIM Karte (Pos. 7) auf der Grundplatte des Routers B-UR-5 (Pos. 1) von der Seite TOP (siehe unten) auszutauschen. Nach dem Austausch der zweiten SIM Karte wird das Gehäuse mit zwei Schrauben (Pos. 6) wieder zusammengeschraubt.

Beispiel für den Adapter für die zweite SIM Karte:



Aufsetzen des Halters für die zweite SIM Karte:



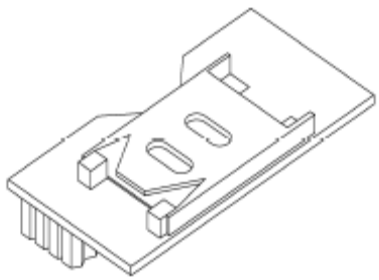
Liste und Beschreibung der Teile

Teil	Beschreibung	Anzahl
1	Grundplatte des UMTS Routers	1
2	Oberer Gehäuseteil des Routers	1
3	Unterer Gehäuseteil des Routers	1
4	Hinterer Frontteil des Routers	1
5	Vorderer Frontteil des Routers	1
6	Schrauben zur Fertigstellung des Gehäuses	2
7	Zweiter Halter der SIM Karte	1

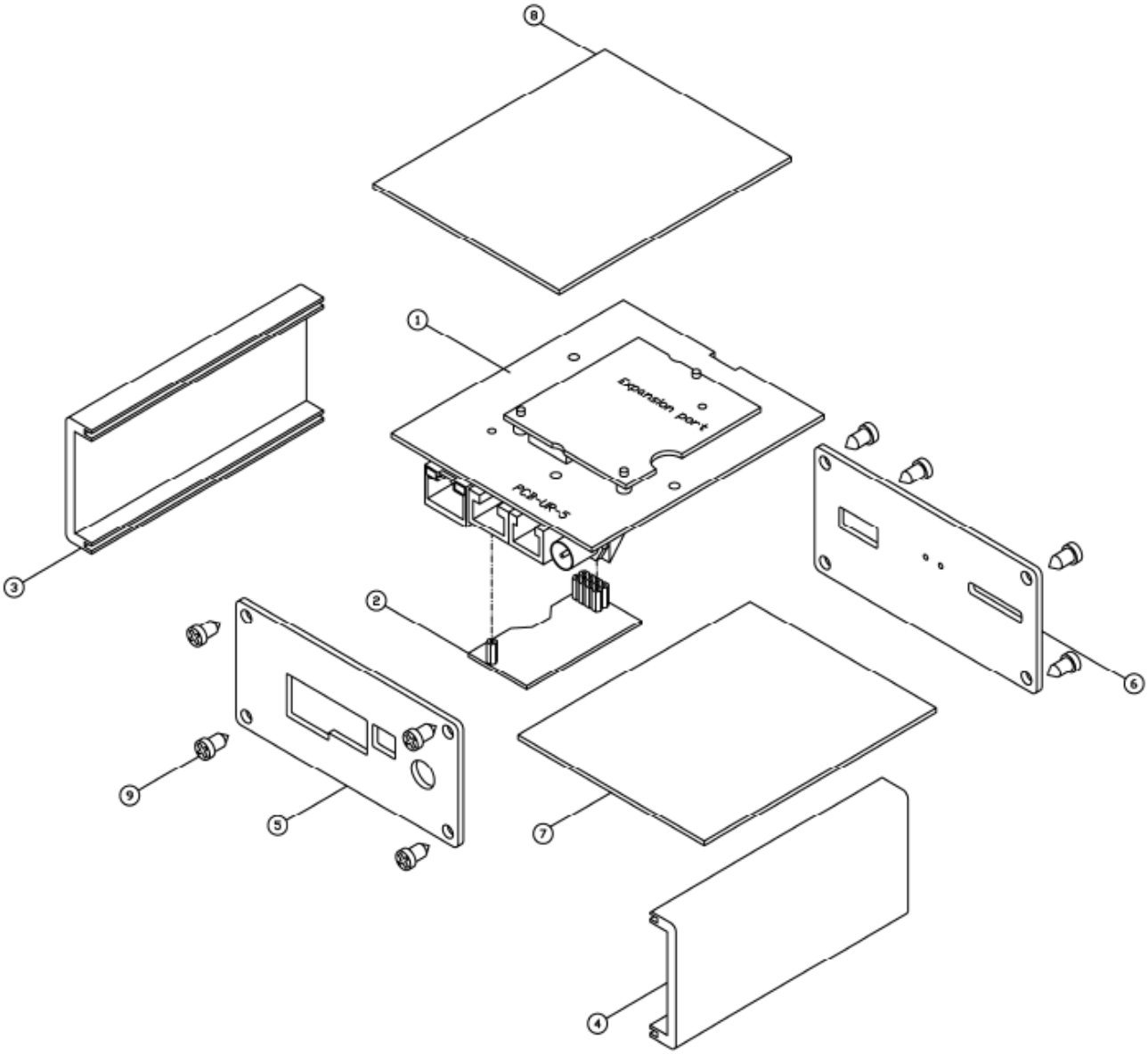
4.2. *Austausch der zweiten SIM Karte beim Router UR 5 SL*

Nach dem Abschrauben von vier Schrauben (Pos. 9) auf der hinteren Frontplatte des Gehäuses (Pos. 5) und nach deren Abnehmen ist es möglich, die SIM Karte (Pos. 7) auf der Grundplatte des Routers B-UR-5 (Pos. 1) von der Seite TOP (siehe unten) auszutauschen. Nach dem Aufsetzen des Anschlusses wird das Gehäuse mit den Schrauben (Pos. 9) wieder zusammengeschraubt.

Beispiel für den Adapter für die zweite SIM Karte:



Aufsetzen des Halters für die zweite SIM Karte:

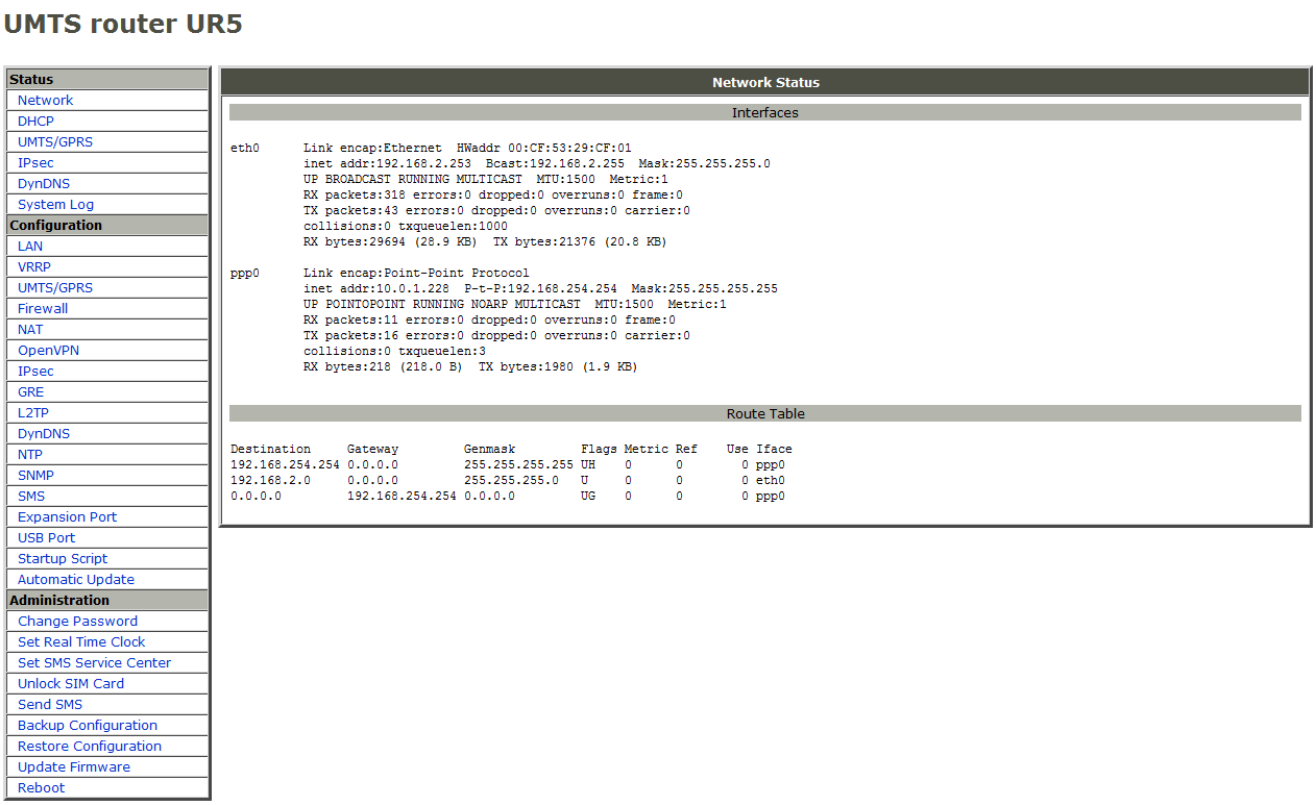


Liste und Beschreibung der Teile

Teil	Beschreibung	Anzahl
1	Grundplatte des UMTS Routers	1
2	Zweiter Halter der SIM Karte	1
3	Linke Seitenwand des Routers	1
4	Rechte Seitenwand des Routers	1
5	Hinterer Frontteil des Routers	1
6	Vorderer Frontteil des Routers	1
7	Unterer Gehäuseteil des Routers	1
8	Oberer Gehäuseteil des Routers	1
9	Schraube zur Fertigstellung des Gehäuses	8

5. Einstellung der Konfiguration über den Webbrowser

Vorsicht! Ohne eingelegte SIM Karte kann der Router nicht betrieben werden. Die eingelegte SIM Karte muss die HSDPA/UMTS/EDGE/GPRS Übertragungen aktiviert haben. Die SIM Karte legen Sie nur dann ein, wenn der Router abgeschaltet ist.
Zur Zustandsüberwachung, Konfiguration und Verwaltung des Routers steht eine Webschnittstelle zur Verfügung. Diese kann durch die Eingabe der IP Adresse des Routers in den Webbrowser aufgerufen werden. Die IP Ausgangsadresse des Routers lautet 192.168.1.1. Die Konfiguration kann nur der Benutzer „Root" mit dem Ausgangspasswort „Root" vornehmen.
Im linken Teil der Webschnittstelle ist das Menü mit der Optionsauswahl der Seiten zur Überwachung des Zustandes (Status), zur Konfiguration (Configuration) und zur Verwaltung (Administration) des Routers untergebracht. Die einzelnen Optonen werden neben dem Menü angezeigt.



Nachdem die LED Diode PWR auf der Fronttafel anfängt zu blinken, ist es möglich, die Ausgangseinstellung des Routers durch die Betätigung der RST Taste wiederherzustellen, damit wird die Wiederherstellung der Konfiguration und das anschließende Reset/Zurücksetzen vorgenommen (grüne LED Diode leuchtet auf).

5.1. *Netzinformationen*

Die Netzinformationen über den Betrieb des Routers können durch die Auswahl der Option *Network* im Menü aufgerufen werden. Im unteren Fensterteil wird die Information über
die Richttabelle angezeigt. Im oberen Fensterteil werden ausführliche Informationen über die
aktiven Schnittstellen angezeigt.

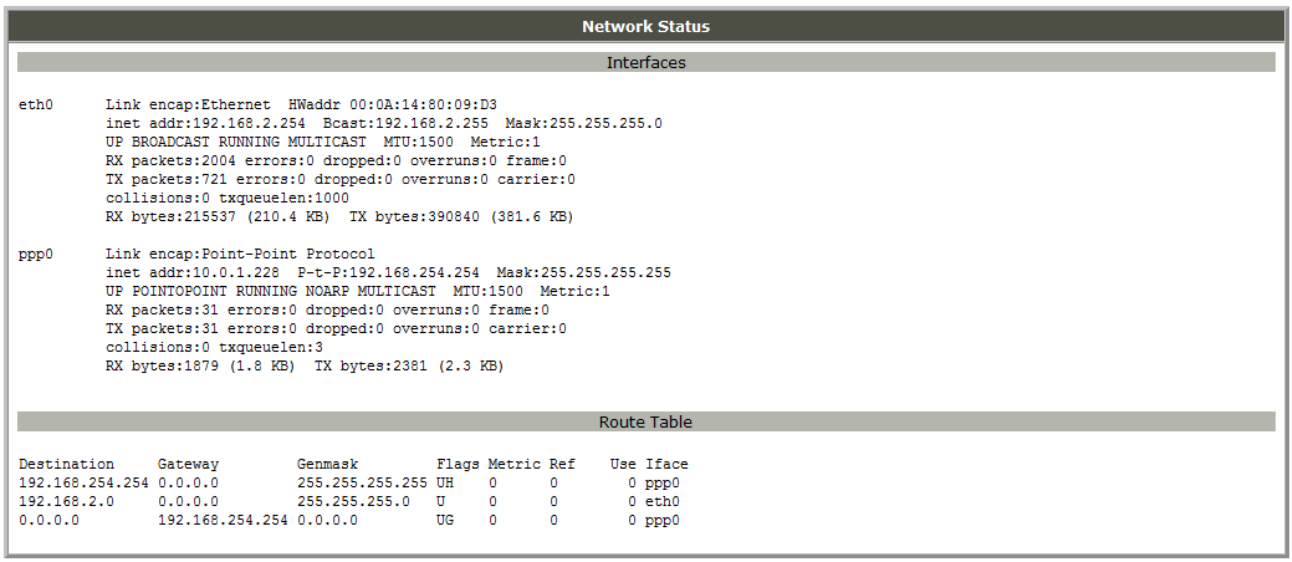
- eth0 – Netzschnittstelle
- ppp0 – PPP Schnittstelle (aktiver Anschluss in GPRS/EDGE/UMTS)

- tun0 – Schnittstelle des OpenVPN Tunnels
- ipsec0 – Schnittstelle des IPsec Tunnels
- gre1 – Schnittstelle des GRE Tunnels

Bei jeder Schnittstelle werden dann folgende Informationen angezeigt:

- HWaddr – (einzigartige) Hardwareadresse der Netzschnittstelle
- inet – eigene IP Adresse
- P-t-P – IP Adresse des gegenüberliegenden Endes der Verbindung
- Bcast – Sendungsadresse
- Mask – Netzmaske
- MTU – maximale Paketgröße, für die das Element das Übertragungsvermögen hat
- Metric – Anzahl der Router, über die das Paket durchgehen muss
- RX packets – empfangene Pakete, Errors – Fehler, Dropped – ausgelassene Pakete
- TX packets – abgesandte Pakete, Errors – Fehler, Dropped – ausgelassene Pa kete
- Collisions – Kollisionen
- RX bytes – Gesamtanzahl der empfangenen Bytes
- TX bytes – Gesamtanzahl der abgesandten Bytes

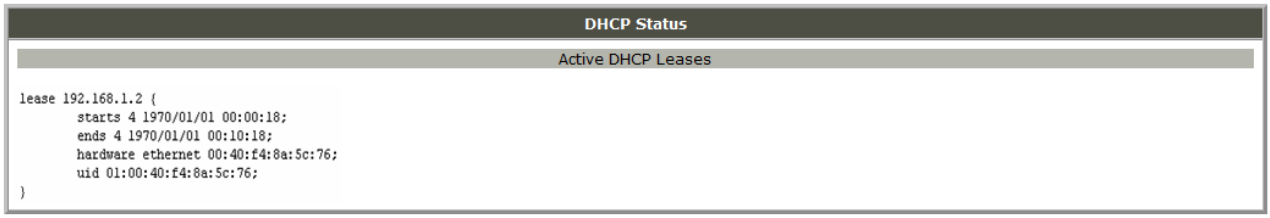
Aus den Netzinformationen ist es möglich, den Zustand der PPP Verbindung abzulesen. Ist die PPP Verbindung aktiv, wird in den Systeminformationen die ppp0 Verbindung angezeigt.


Network Status
Interfaces
eth0 Link encap:Ethernet HWaddr 00:0A:14:80:09:D3
inet addr:192.168.2.254 Bcast:192.168.2.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2004 errors:0 dropped:0 overruns:0 frame:0
TX packets:721 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:215537 (210.4 KB) TX bytes:390840 (381.6 KB)
ppp0 Link encap:Point-Point Protocol
inet addr:10.0.1.228 P-t-P:192.168.254.254 Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:31 errors:0 dropped:0 overruns:0 frame:0
TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:3
RX bytes:1879 (1.8 KB) TX bytes:2381 (2.3 KB)
Route Table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.254.254 0.0.0.0 255.255.255.255 UH 0 0 0 ppp0
192.168.2.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
0.0.0.0 192.168.254.254 0.0.0.0 UG 0 0 0 ppp0

5.2. *DHCP Status*

Die Informationen über die vom DHCP Server dem Router UR R zugeteilten IP Adressen sind im Menü in der Option DHCP zu finden:

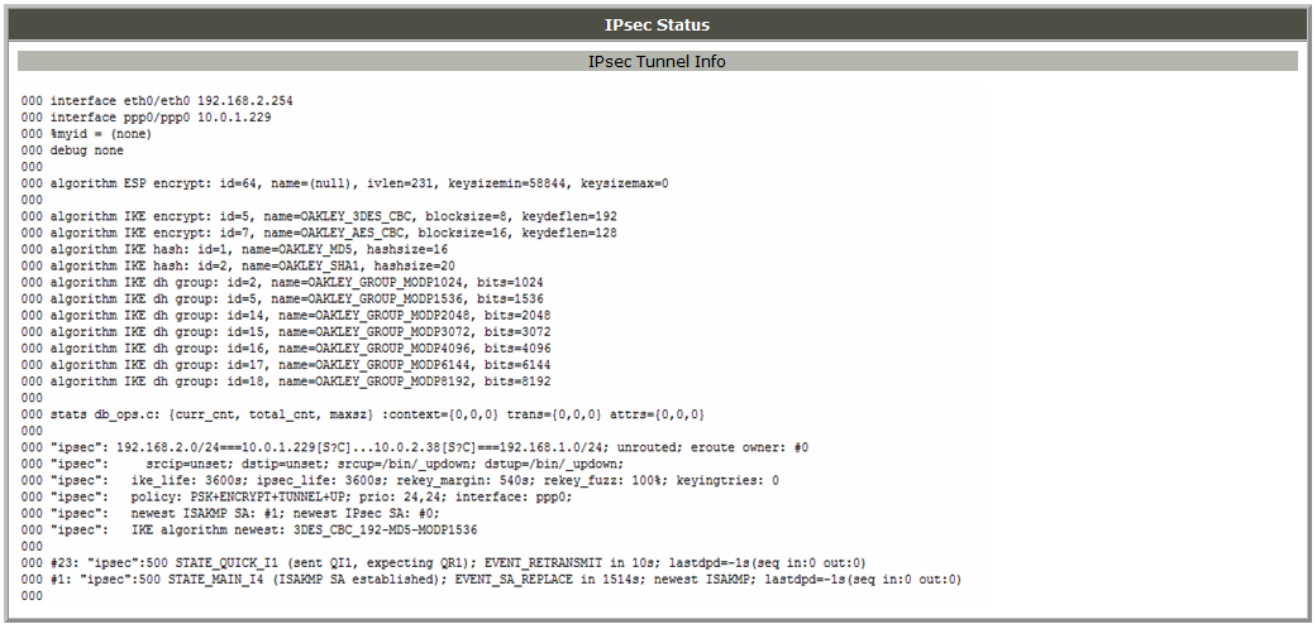
- lease 192.168.1.2 (im allgemeinen IP Adresse) – zugeteilte IP Adresse
- starts – die Zeit der Zuteilung der IP Adresse
- ends – Dauer der Gültigkeit der zugeteilten IP Adresse
- hardware ethernet – (einzigartige) Hardwareadresse MAC
- uid – einzigartige ID Nummer



Im Grenzfall kann der DHCP Status zu einer IP Adresse zwei DHCP Zustände anzeigen, die Ursache dafür kann das Zurücksetzen der Netzkarte sein.

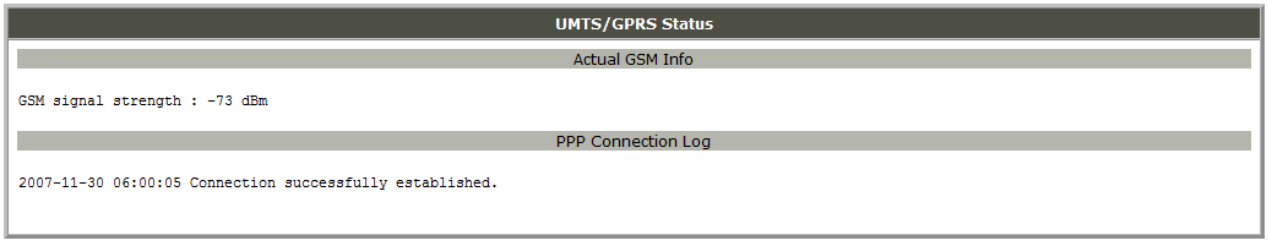
5.3. *IPsec Status*

Die Informationen über den aktuellen Zustand des IPsec Tunnels können durch Auswahl der Option IPsec im Menü aufgerufen werden. Die genaue Beschreibung der hier angezeigten Informationen finden Sie auf http://www.freeswan.org/doc.html.

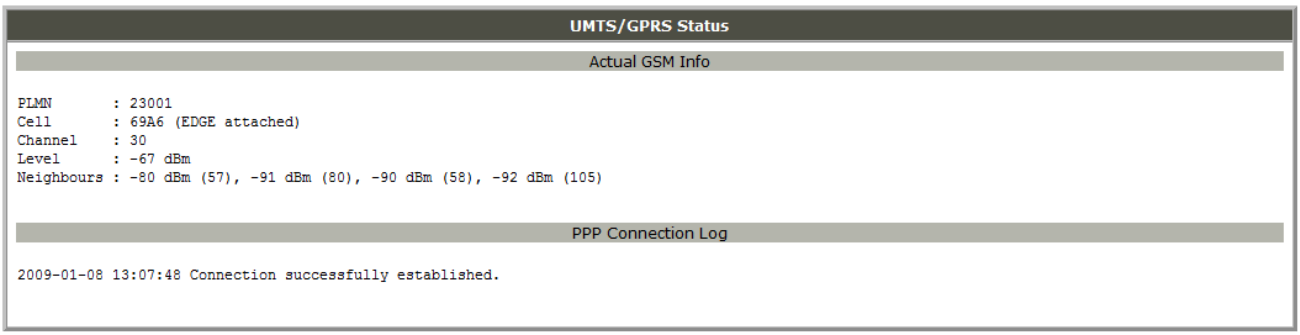

IPsec Status
IPsec Tunnel Info
000 interface eth0/eth0 192.168.2.254
000 interface ppp0/ppp0 10.0.1.229
000 %myid = (none)
000 debug none
000
000 algorithm ESP encrypt: id=64, name=(null), ivlen=231, keysizemin=58844, keysizemax=0
000
000 algorithm IKE encrypt: id=5, name=OAKLEY_3DES_CBC, blocksize=8, keydeflen=192
000 algorithm IKE encrypt: id=7, name=OAKLEY_AES_CBC, blocksize=16, keydeflen=128
000 algorithm IKE hash: id=1, name=OAKLEY_MD5, hashsize=16
000 algorithm IKE hash: id=2, name=OAKLEY_SHA1, hashsize=20
000 algorithm IKE dh group: id=2, name=OAKLEY_GROUP_MODP1024, bits=1024
000 algorithm IKE dh group: id=5, name=OAKLEY_GROUP_MODP1536, bits=1536
000 algorithm IKE dh group: id=14, name=OAKLEY_GROUP_MODP2048, bits=2048
000 algorithm IKE dh group: id=15, name=OAKLEY_GROUP_MODP3072, bits=3072
000 algorithm IKE dh group: id=16, name=OAKLEY_GROUP_MODP4096, bits=4096
000 algorithm IKE dh group: id=17, name=OAKLEY_GROUP_MODP6144, bits=6144
000 algorithm IKE dh group: id=18, name=OAKLEY_GROUP_MODP8192, bits=8192
000
000 stats db_ops.c: {curr_cnt, total_cnt, maxsz} :context={0,0,0} trans={0,0,0} attrs={0,0,0}
000
000 "ipsec": 192.168.2.0/24===10.0.1.229[S?C]...10.0.2.38[S?C]===192.168.1.0/24; unrouted; eroute owner: #0
000 "ipsec":   srcip=unset; dstip=unset; srcup=/bin/_updown; dstup=/bin/_updown;
000 "ipsec":   ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
000 "ipsec":   policy: PSK+ENCRYPT+TUNNEL+UP; prio: 24,24; interface: ppp0;
000 "ipsec":   newest ISAKMP SA: #1; newest IPsec SA: #0;
000 "ipsec":   IKE algorithm newest: 3DES_CBC_192-MD5-MODP1536
000
000 #23: "ipsec":500 STATE_QUICK_I1 (sent QI1, expecting QR1); EVENT_RETRANSMIT in 10s; lastdpd=-1s(seq in:0 out:0)
000 #1: "ipsec":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 1514s; newest ISAKMP; lastdpd=-1s(seq in:0 out:0)
000

5.4. *UMTS/GPRS Status*

Beinhaltet der Router das Modul Cinterion HC15, enthält die Option *PPP* im Menü die Information über die Signalstärke. Im unteren Teil dieses Fensters ist *PPP Connection Log*, wo Informationen über den Verbindungsaufbau und über etwaige Probleme bei der Herstellung der Verbindung zu finden sind.

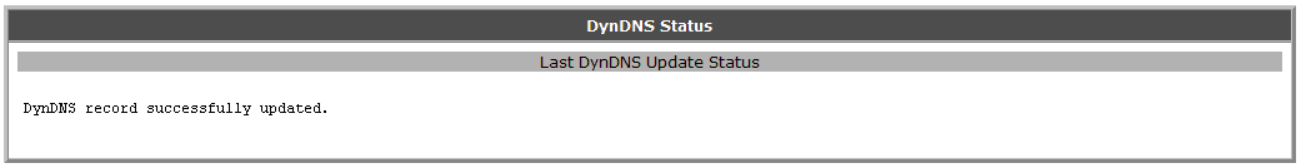


Beinhaltet der Router das Modul Cinterion HC25, enthält die Option *PPP* im Menü die aktuellen Informationen über PLMN (Netzbetreibercode), über die Zelle, den Kanal und die Signalqualität der ausgewählten Zelle sowie der anliegenden vernehmbaren Zellen. Im unteren Teil dieses Fensters werden Informationen über den Aufbau der GPRS Verbindung und über etwaige Probleme bei der Herstellung dieser Verbindung angezeigt.


UMTS/GPRS Status
Actual GSM Info
PLMN : 23001
Cell : 69A6 (EDGE attached)
Channel : 30
Level : -67 dBm
Neighbours : -80 dBm (57), -91 dBm (80), -90 dBm (58), -92 dBm (105)
PPP Connection Log
2009-01-08 13:07:48 Connection successfully established.

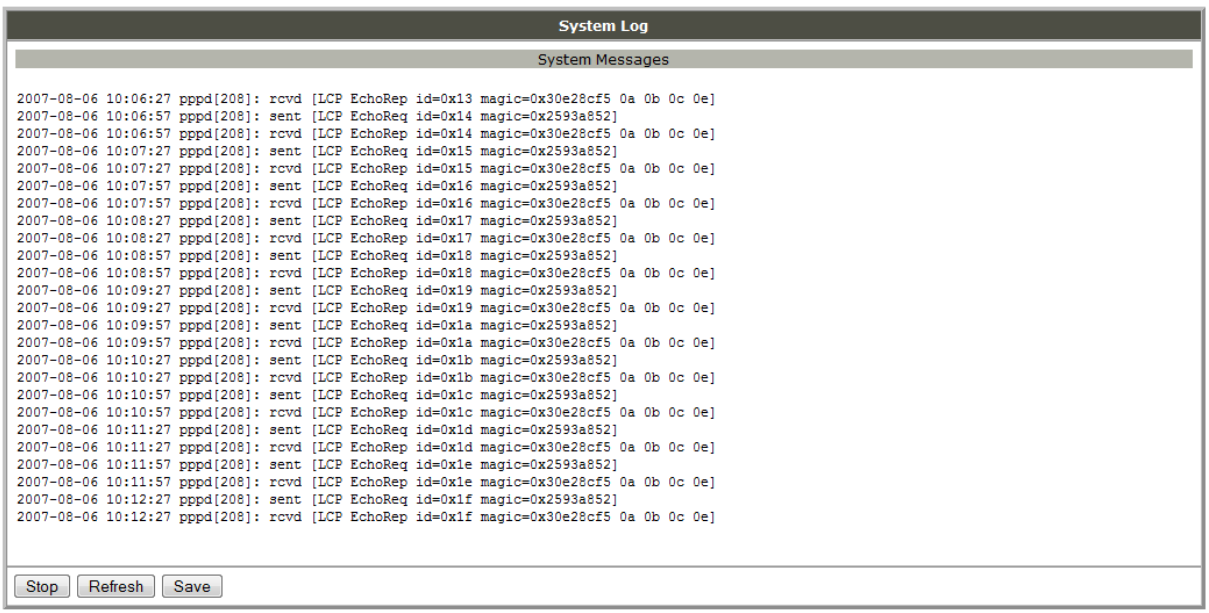
5.5. *DynDNS Status*

Das Ergebnis der Aktualisierung der DynDNS Aufzeichnung am Server www.dyndns.org kann durch die Auswahl der Option DynDNS im Menü aufgerufen werden.



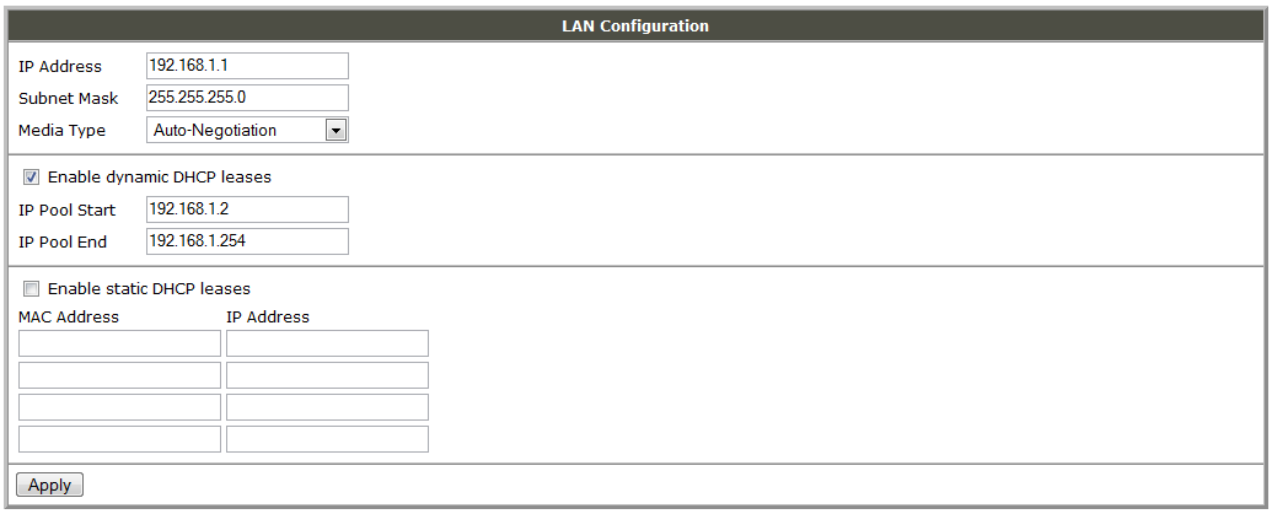
5.6. *System Log*

Im Falle von Problemen beim Aufbau der PPP Verbindung kann das System Log durch die Auswahl der Option *System Log* im Menü aufgerufen werden. Im Fenster werden die ausführlichen Meldungen von einzelnen im Router laufenden Anwendungen angezeigt. Der Fensterinhalt kann durch die Betätigung der Taste *Refresh* aktualisiert werden. Mit der *Save* Taste ist es möglich System Log zu speichern.

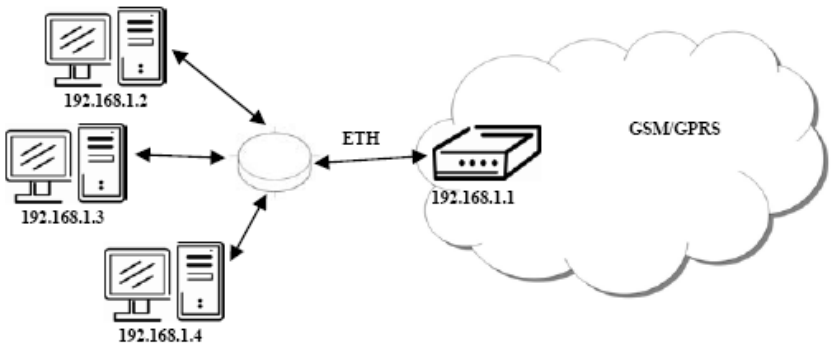


5.7. *Konfiguration der Netzschnittstelle*

Die Konfiguration der Netzschnittstelle kann durch Auswahl der Option *LAN im Menü* aufgerufen werden. Im ersten Fensterteil können die eigene IP Adresse der Netzschnittstelle *(IP Address)*, die Netzmaske *(Subnet Mask)* und der Mediumtyp *(Media type)* definiert werden, in den meisten Fällen funktioniert *Auto-Negotiation*.
Im zweiten Fensterteil kann der DHCP Server durch das Ankreuzen der Option *Enable dynamic DHCP leases* freigegeben werden. Im Fenster kann der Anfang *(IP Pool Start)* und das Ende *(IP Pool End)* des Bereichs von IP Adressen, die den DHCP Klienten zugeteilt werden, definiert werden. Wird die Option *Enable dynamic DHCP leases* nicht angekreuzt, teilt der Router die IP Adressen nicht zu.
Im dritten Fensterteil ist es möglich, durch das Ankreuzen der Option *Enable static DHCP leases* die Zuteilung von bis zu vier statischen IP Adressen *(IP Address),* die den MAC Adressen *(MAC Address)* der angeschlossenen Geräte, Stationen usw. entsprechen, zu definieren.
Die Änderungen der Einstellungen wirken sich nach der Betätigung der Apply Taste aus.
Der DHCP Server teilt den angeschlossenen Kunden die IP Adressen des definierten Adressenbereiches, die IP Gatewayadresse und IP Adresse des DNS Servers zu. Es ist wichtig, dass sich die Bereiche der statisch vorgegebenen IP Adressen und der vom DHCP zugeteilten Adressen nicht überlappen, ansonsten kann eine Adressenkollision und somit eine falsche Netzfunktion auftreten.



Beispiel für die Einstellung der Netzschnittstelle mit dynamischem DHCP Server:



LAN Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Media Type	Auto-Negotiation

☑ Enable dynamic DHCP leases

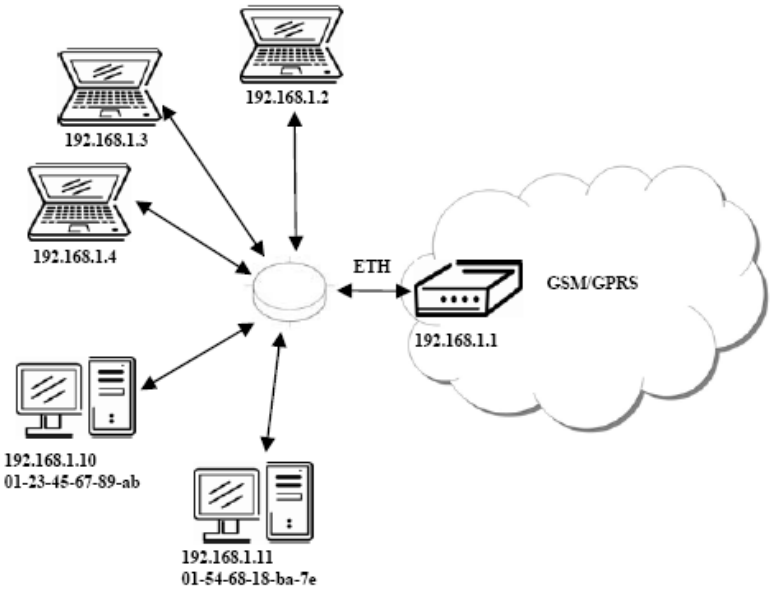
IP Pool Start	192.168.1.2
IP Pool End	192.168.1.4

☐ Enable static DHCP leases

MAC Address	IP Address

Apply

Beispiel für die Einstellung der Netzschnittstelle mit dem dynamischen und statischen HCP Server:



LAN Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Media Type	Auto-Negotiation

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.1.2
IP Pool End	192.168.1.4

☑ Enable static DHCP leases

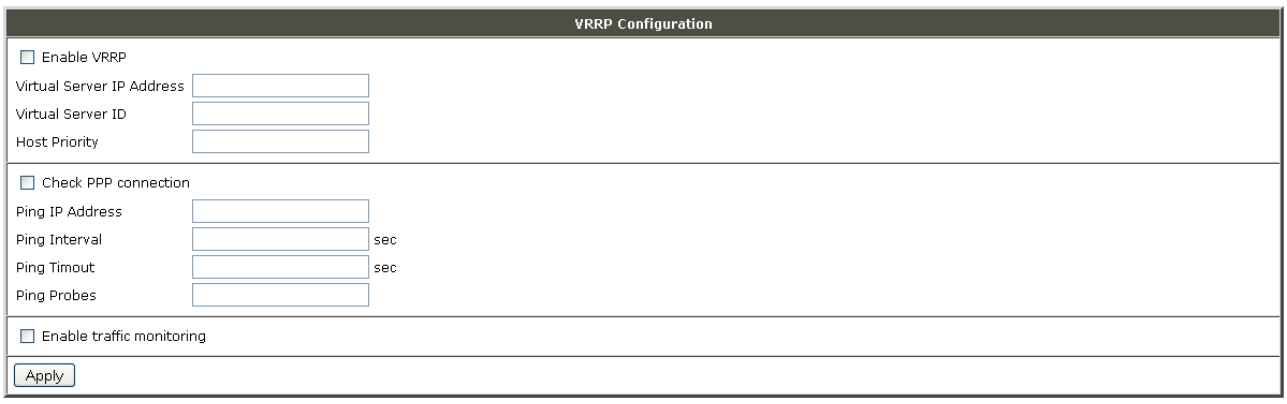
MAC Address	IP Address
01:23:45:67:89:ab	192.168.1.10
01:54:68:18:ba:7e	192.168.1.11

Apply

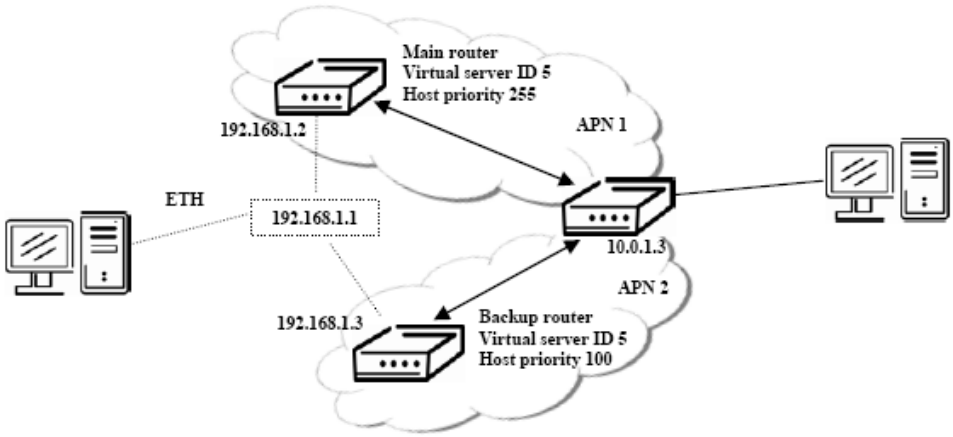
5.8. *VRRP Konfiguration*

Die VRRP Konfiguration kann durch die Auswahl der Option VRRP im Menü aufgerufen werden. Das Protokoll VRRP (Virtual Router Redundancy Protocol) ist eine Technik, mittels der es möglich ist, die Richtpflichten von einem Hauptrouter auf einen anderen Reserverouter zu übertragen, falls der Hauptrouter versagt. Das Protokoll VRRP kann durch das Ankreuzen der Option *Enable VRRP* freigegeben werden. Der Parameter *Virtual Server IP Address* stellt die IP Adresse des virtuellen Servers ein, diese Adresse ist für beide Router gleich. Das angeschlossene Gerät sendet seine Daten über diese virtuelle Adresse. Sollten im Netz mehrere virtuelle Router bestehen, unterscheidet der Parameter *Virtual Server ID* diese virtuelle Router voneinander. Beim Haupt- und beim Reserverouter muss dieser Parameter gleich eingestellt werden. Zum Hauptrouter wird der Router, der die mit dem Parameter *Host Priority* höhere Priorität eingestellt hat. In Abhängigkeit von RFC 2338 hat der Hauptrouter die höchstmögliche Priorität, und zwar 255. Der Reserverrouter hat die Priorität im Grenzbereich 1 – 254 (Ausgangswert ist 100). Der Wert der Priorität gleich 0 ist nicht erlaubt.

Im zweiten Fensterteil kann die Kontrolle des Verbindungsaufbaus über PPP (GPRS) durch das Ankreuzen der Option *Check PPP connection* gewählt werden. Der aktive Hauptrouter (Haupt-/Reserverouter) sendet dann selbst die Ping Abfragen an die angeführte IP Adresse *(Ping IP Address)* in regelmäßigen Zeitintervallen (Ping Interval) mit eingestellter Wartezeit auf die Antwort *(Ping Timeout)*. Die Kontrolle der PPP Verbindung ist zur Erkennung der Durchgängigkeit auf der Trasse vorgesehen, auf deren Grundlage die Übertragung der Routerfunktion vom Haupt- auf den Reserverouter, bzw. umgekehrt erfolgt. Die Trasse wird für undurchgängig gehalten, falls auf die festgesetzte Anzahl der Ping Abfragen *(Ping Probes)* keine Antwort zurückkommt. Als Ping Adresse muss die IP Adresse benutzt werden, bei der sicher ist, dass sie immer erreichbar bleibt und an die es möglich ist, die ICMP Abfragen (z. B. des DNS Server Netzbetreibers) zu senden. Zur Überwachung der Durchgängigkeit auf der Trasse ist es auch möglich, den Parameter *Enable traffic monitoring* zu nutzen. Ist dieser Parameter eingestellt, wird dann, falls ein anderes Paket als Ping auf die überwachte Trasse ausgesendet wird, inspiziert, ob irgendeine Antwort bis zum Ping Timeout zurückkommt. Ist dies nicht der Fall, wird die ursprüngliche ausgesendete Nachricht für eine Prüfnachricht (als ob Ping ausgesendet worden wäre, worauf keine Antwort zurückgekommen ist) gehalten und dann erfolgt eine beschleunigte Prüfung (mit einem Intervall zwischen der Aussendung, das durch den Parameter *Ping Timeout* gegebenen ist) mittels der Ping Nachrichten, wobei die erste ausgesendete Ping Nachricht schon als die zweite Prüfnachricht in Reihe gilt, die mit dem Parameter *Ping Probes* begrenzt wird.



Beispiel für die Einstellung des VRRP Protokolls:



VRRP Configuration

Enable VRRP	
Virtual Server IP Address	192.168.1.1
Virtual Server ID	5
Host Priority	255
Check PPP connection	
Ping IP Address	10.0.1.3
Ping Interval	10 sec
Ping Timout	5 sec
Ping Probes	10
Enable traffic monitoring	

Apply

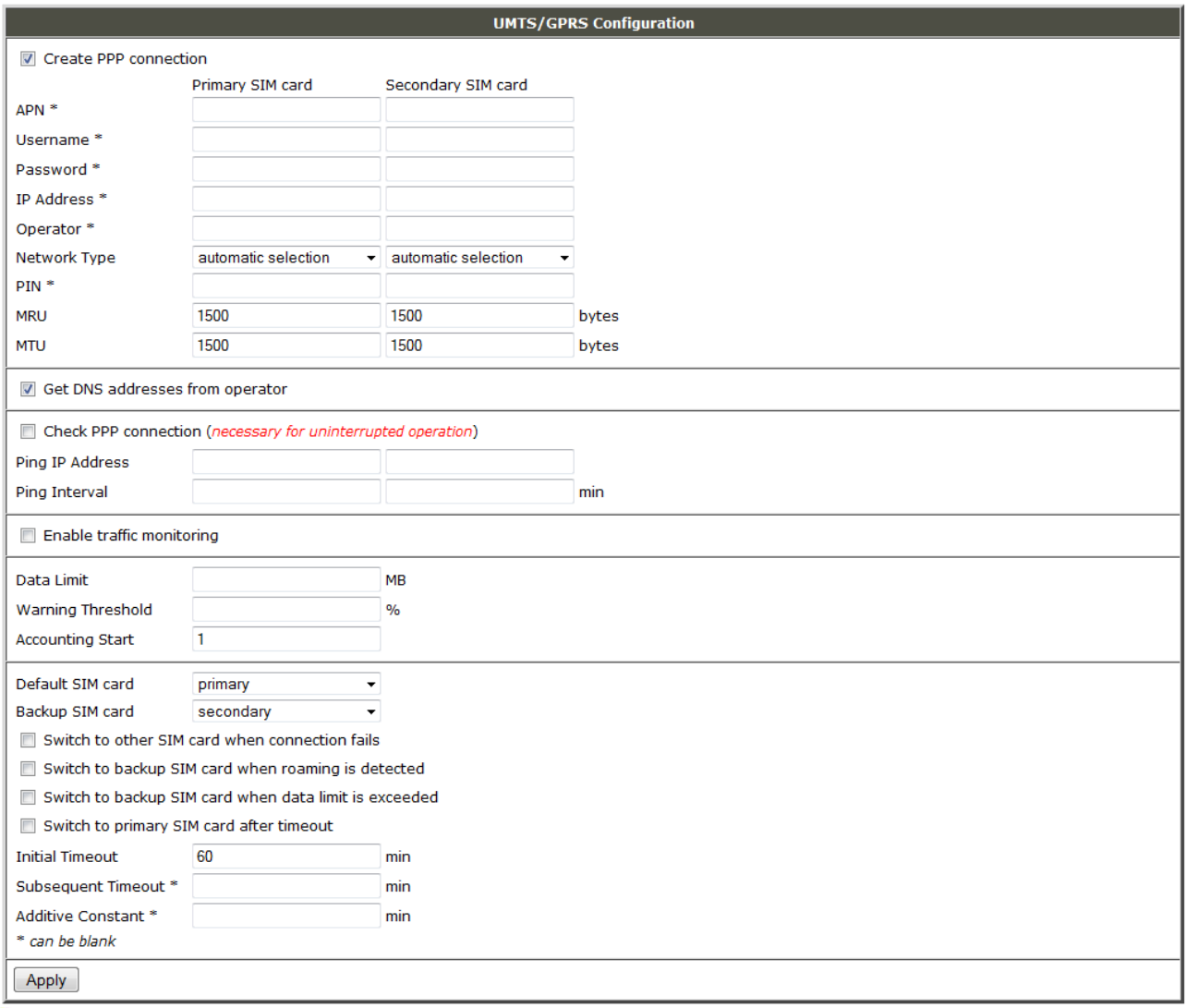
5.9. *Konfiguration des Verbindungsaufbaus in UMTS/GPRS*

Die Konfiguration des Verbindungsaufbaus in UMTS/GPRS kann durch die Auswahl der Option *UMTS/GPRS* im Menü aufgerufen werden. Ist die Option *Create PPP connection* angekreuzt, versucht der Router selbst nach dem Einschalten die PPP Verbindung herzustellen. Im Fenster können *APN*, Benutzername (*Username*), Zutrittspasswort (*Password*), IP Adresse (*IP Address*) und PIN (*PIN*) für zwei SIM Karten, bzw. falls die erste SIM Karte zwei verschiedene APN eingestellt hat, definiert werden. Falls das Feld *IP Address* nicht ausgefüllt wird, wird die IP Adresse beim Verbindungsaufbau automatisch vom Netzbetreiber zugeteilt. Durch Ausfüllung der vom Netzbetreiber zur Verfügung gestellten IP Adresse wird der Anschluss des Routers ans Netz beschleunigt.

Falls das Feld *APN* unausgefüllt bleibt, wählt der UR5 Router APN automatisch laut dem IMSI Code der SIM Karte aus. Falls PLMN (Netzbetreibercode) nciht in der APN Liste ist, wird die Ausgangs-APN „Internet“ genutzt. APN wird vom Mobilnetzbetreiber definiert. Der Parameter PLMN kann in der Option *Operator* definiert werden. Die Option *Network Type* definiert die Weise der Datenübertragung, und zwar die automatische Auswahl in Abhängigkeit von der Netzverfügbarkeit oder durch die *UMTS/HSDPA* oder *GPRS/EDGE* Technologie. Mit dem Parameter *PIN* ist es möglich, den PIN Code in die SIM Karte bei jedem Start des Routers UR5 einzugeben.

Vorsicht! Steckt nur eine SIM Karte im Router UR5 die zwei verschiedene APN eingestellt hat, darf der Router UR5 keinen aufgesetzten Halter für die zweite SIM Karte haben, ansonsten erfolgt keine richtige Umschaltung auf die zweite im Webformular definierte APN. Auch muss der richtige PIN Code angegeben werden, für die SIM Karte mit zwei APN ist PIN gleich für die beiden APN, ansonsten kann es zum Sperren der SIM Karte durch die mehrfache Eingabe des falschen PIN Codes kommen.

Die Auswahl der Option *Get DNS Address from Operator* ist für die einfachere Konfiguration auf Seiten des Kunden bestimmt. Ist diese Option angekreuzt, versucht der Router die IP Adressen des primären und sekundären DNS Servers vom Netzbetreiber automatisch zu ermitteln.
Ist die *Option Check PPP Connection* angekreuzt, wird die Kontrolle des Verbindungsaufbaus über PPP aktiviert. Der Router sendet dann selbst die Ping Abfragen an die angeführte IP Adresse *(Ping IP Address)* in regelmäßigen Zeitintervallen *(Ping Interval)*. Gelingt es nicht, Ping an die angeführte IP Adresse 3x nacheinander zu senden, beendet der Router die bestehende Verbindung und versucht eine neue herzustellen. Die Kontrolle kann separat für zwei SIM Karten oder für zwei APN eingestellt werden. Als Ping Adresse kann die IP Adresse benutzt werden, bei der sicher ist, dass sie immer funktionsfähig bleibt und an die es möglich ist die ICMP Ping Abfragen (z. B. DNS Server des Netzbetreibers) zu senden.
Ist die Funktion *Enable Traffic Monitoring* angekreuzt, hört der Router auf, die Ping Abfragen an die *Ping IP Address* zu senden und überwacht den PPP Verbindungsaufbau. Beim Nullbetrieb in einem Zeitintervall, der länger als der Ping Interval ist, sendet der Router eine Abfrage an die Adresse *Ping IP Address*.
Der Parameter *Data Limit* stellt den Grenzwert der Datensendung über GPRS ein. Mit dem Parameter *Accounting Start* ist es möglich zu präzisieren, nach welcher Datenmenge die im Parameter *Data Limit* eingestellte Verrechnung gestartet wird. Ist der Parameter *Switch to Backup SIM Card When Data Limit Is Exceeded* (siehe unten) oder *Send SMS When Data Limit Is Exceeded* (siehe SMS Konfiguration) nicht angekreuzt, wird der Datengrenzwert nicht berechnet.
Der Parameter *Warning Threshold* gibt den prozentualen Wert des Parameters *Data Limit* an, nach dessen Überschreitung der Router eine SMS in der Form Router has exceeded (Wert des Parameters *Warning Threshold*) of Data Limit sendet.
Im Unterteil der Konfiguration ist es möglich, die Regeln zum Umschaltung zwischen zwei SIM Karten bzw. zwischen zwei APN auf einer SIM Karte einzustellen. Der Parameter *Default SIM Card* stellt die Ausgangs-APN oder Ausgangs-SIM Karte ein, von der aus versucht wird die PPP Verbindung aufzubauen. Bei Einstellung dieses Parameters auf *None* startet der Router im Modus Offline und die PPP Verbindung muss mittels einer SMS Nachricht aufgebaut werden. Beim Ausfall der PPP Verbindung stellt der freigegebene Parameter *Switch to Other SIM Card When Connection Fails* das Umschalten auf die zweite SIM Karte oder die zweite APN sicher. Falls das Roaming erfasst wird, ermöglicht der Parameter *Switch to Backup SIM Card When Roaming Is Detected* das Umschalten auf die zweite SIM Karte oder zweite APN. Der Parameter *Switch to Backup SIM Card When Data Limit Is Exceeded* stellt das Umschalten auf die zweite SIM Karte oder zweite APN im Falle der Überschreitung des Datengrenzwertes, der im Parameter *Data Limit* eingestellt wurde. Mit dem Parameter *Switch to Primary SIM Card after Timeout* ist es möglich, die Art zu definieren, auf welche der Router versucht zurück auf die Ausgangs-SIM Karte oder Ausgangs-APN umzuschalten.
Der Parameter *Initial Timeout* stellt die Zeit ein, nach deren Ablauf der Router versucht von der zweiten APN auf die Ausgangs-APN zurück zu schalten, der Bereich dieses Parameters beträgt 1 bis 10 000 Minuten. Der Parameter *Subsequent Timeout* stellt die Zeitperiode des Versuches ein, eine weitere Anmeldung zur Ausgangs-APN zu realisieren, der Bereich beträgt 1 bis 10 000 Minuten. Der Parameter *Additive Constant* gibt die Zeit ein, um welche die Zeit beim Versuch, die Hauptverbindung herzustellen, nach dem als
erfolglosen definierten Versuch verlängert wird (z. B. nach dem zweiten erfolglosen Versuch die Hauptverbindung aufzubauen, wird die Zeit des weiteren Versuchs um 30 Minuten verlängert usw.). Der Bereich beträgt 1 bis 1 000 Minuten.
Die Änderungen der Einstellungen wirken sich nach Betätigung der Taste *Apply* aus.



Attention! We recommend checking the GPRS connection in case of uninterrupted running.

Anmerkung:

- MTU (Maximum Transmission Unit) – identifiziert die maximale Paketgröße, für die das Element in der gegebenen Umgebung das Übertragungsvermögen hat. Vom Herstellerwerk ist die Größe auf 1 500 Bytes eingestellt..
- MRU (Maximum Receiving Unit) – identifiziert die maximale Paketgröße, für die das Element in der gegebenen Umgebung das Empfangsvermögen hat. Vom Herstellerwerk ist die Größe auf 1 500 Bytes eingestellt.
  Bei der Einstellung einer fehlerhaften Größe kann es vorkommen, dass die Datenübertragung nicht korrekt verläuft.

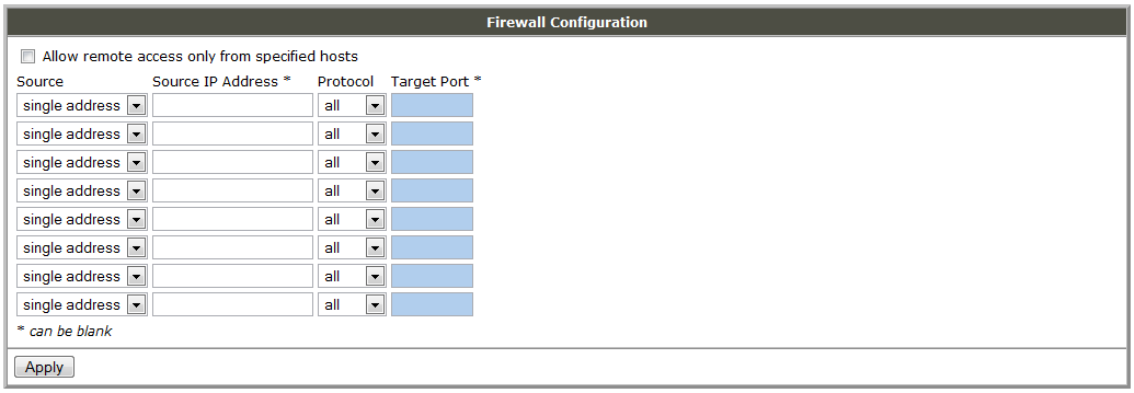
5.10. *Firewall Konfiguration*

Mit der Firewall können die IP Adressen eingestellt werden, von denen der Fernzutritt zum Router möglich ist. Die Auswahl der Option *Allow Remote Access Only from Specified Hosts* schaltet die Firewall ein/aus. In der Firewall ist es möglich, bis zu acht Fernzutritte mittels der Parameter *Source, Source IP Address, Protocol* und *Target Port* einzustellen.

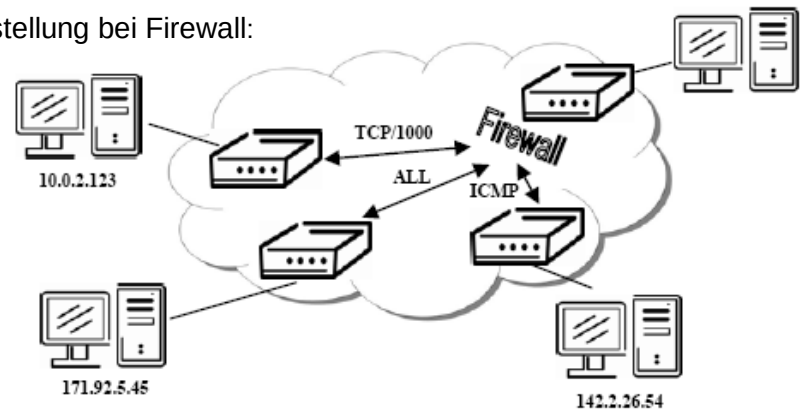
Der Parameter *Source* definiert, ob der Zutritt der einzigen IP Adresse, die als *Source IP Address* definiert wird, oder jeder beliebigen IP Adresse freigegeben wird. Im Menü *Protocol* ist es möglich zu präzisieren mit welchem Protokoll der Zutritt freigegeben wird, es kann der Zutritt für alle Protokolle *(all)* oder für die Protokolle *UDP*, *TCP* oder I*CMP* gewählt werden. Mit dem Parameter *Target Port* ist es möglich, die Anschlussnummer ausführlicher einzustellen.

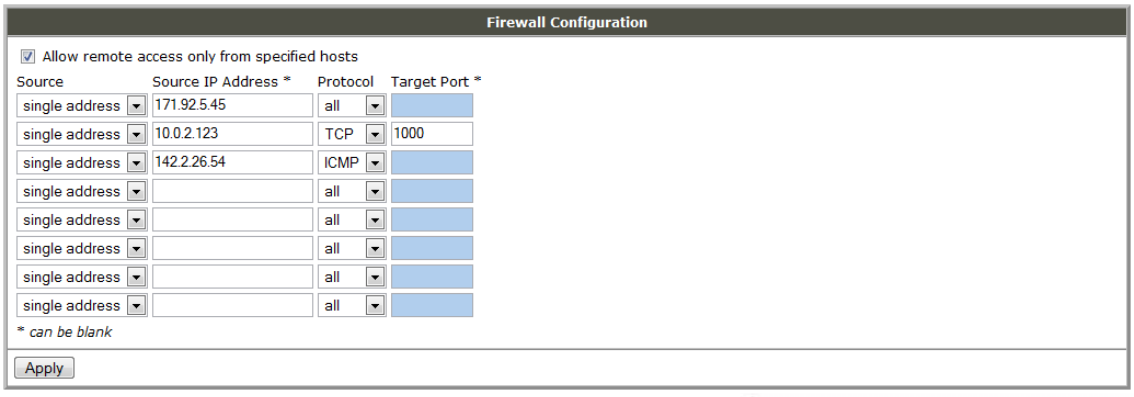
Die Änderungen der Einstellungen wirken sich nach der Betätigung der Apply Taste aus.

Vorsicht! Firewall filtriert nicht die Verbindung über Ethernet.



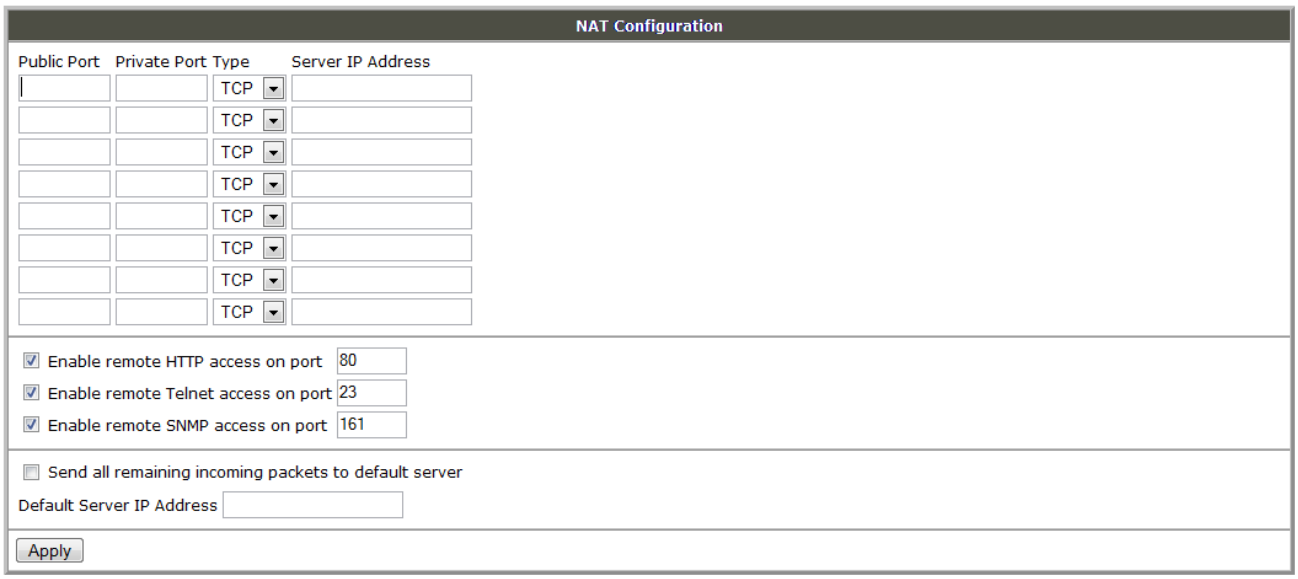
Beispiel für die Einstellung bei Firewall:



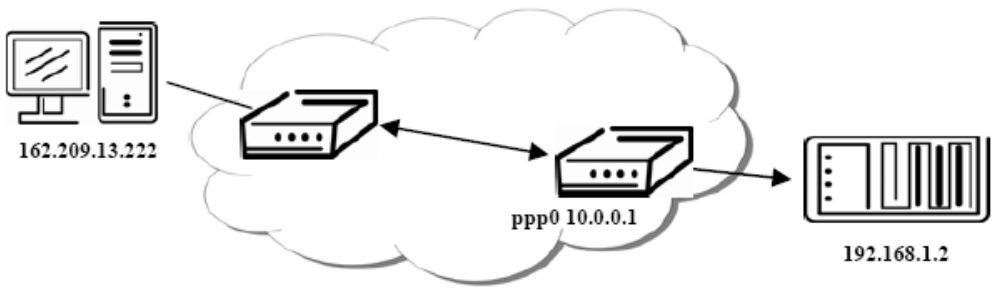


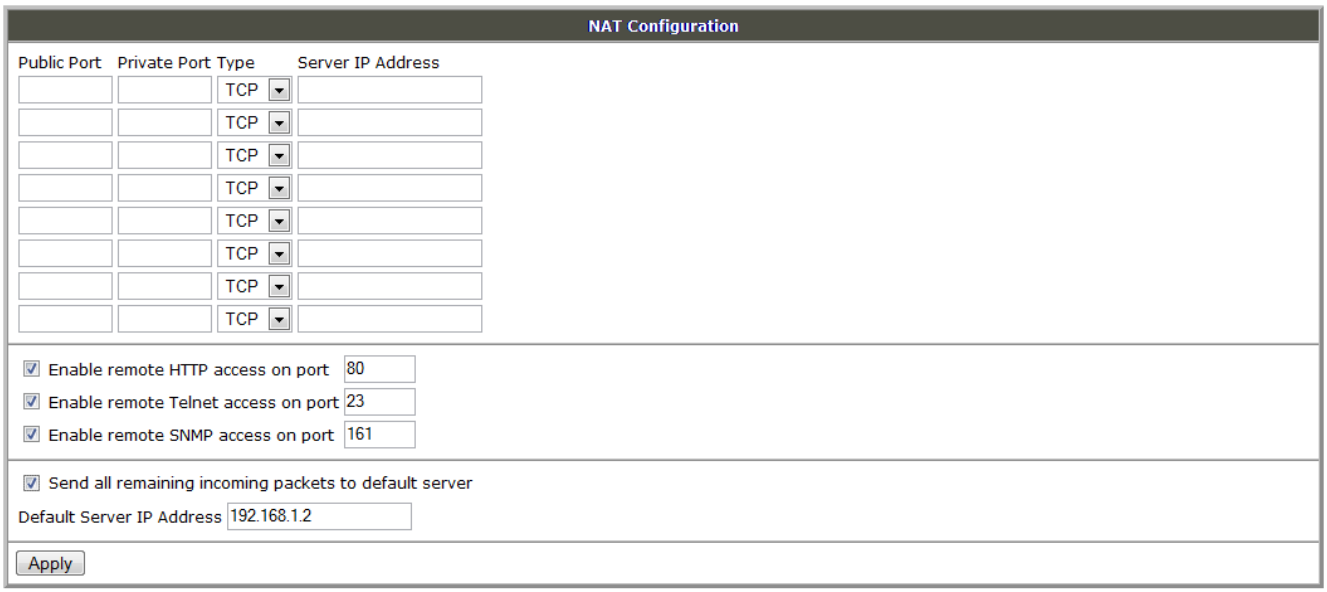
5.11. *Konfiguration der Adressenübersetzung (NAT)*

Die Konfiguration der Adressenübersetzung kann durch die Auswahl der Option NAT im Menü aufgerufen werden. Das Fenster beinhaltet acht Optionen zur Bestimmung der Adressenübersetzung, jede Zeile enthält den Außenanschluss, Innenanschluss, die Auswahl des Protokolls TCP/UDP und die IP Adresse, an die die ankommenden Daten gesandt werden.
Durch das Ankreuzen der Option *Send All Incoming Packets to Default Server* und durch die Einstellung der Option *Default Server* kann der Router in einen Modus gebracht werden, in dem er die sämtliche ankommende Kommunikation von PPP an einen Computer mit definierter IP Adresse weiterleitet.
Durch das Ankreuzen der Option *Enable Remote http Access* on Port und durch die Eingabe der Anschlussnummer ist es möglich, die Konfiguration des Routers über eine Webschnittstelle vorzunehmen.
Die Auswahl der Option *Enable RemoteTelnet Access* on Port und die Eingabe der Anschlussnummer ermöglichen den Zutritt über *Telnet*.
Die Auswahl der Option *Enable Remote SNMP Access on Port* und Eingabe der Anschlussnummer bietet die Möglichkeit der Abfragen des SNMP Agenten frei.
Die Änderungen der Einstellungen wirken sich nach Betätigung der Taste *Apply* aus.



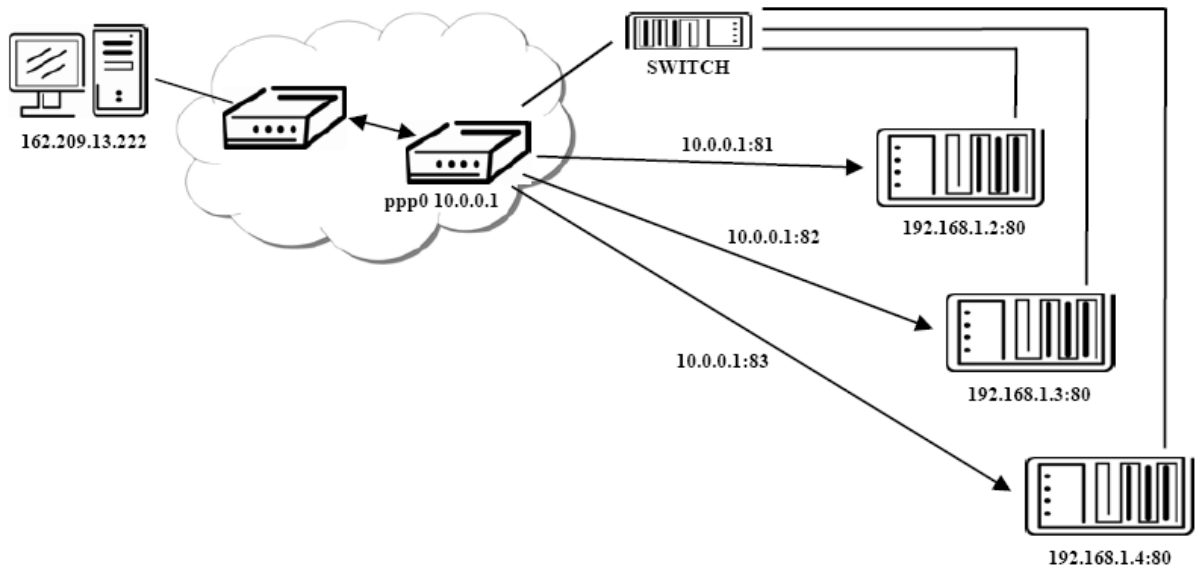
Beispiel für die Konfiguration mit einem an den Router angeschlossenen Gerät:

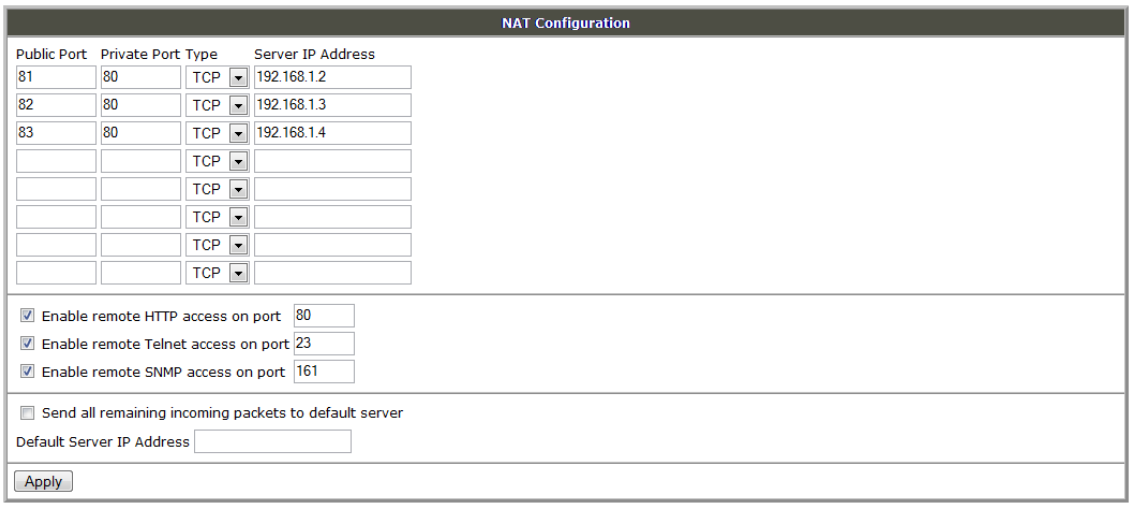




Bei dieser Konfiguration ist es wichtig, die Option *Send All Remaining Incoming Packets to Default Server* gekennzeichnet zu haben, die IP Adresse ist in diesem Falle die Adresse des hinter den Router angeschlossenen Gerätes. Das hinter den Router angeschlossene Gerät muss das Ausgangsgateway auf den Router eingestellt haben. Bei PING an die IP Adresse der SIM Karte antwortet das angeschlossene Gerät.

Beispiel für die Konfiguration mit mehreren Geräten am Router:





Bei dieser Konfiguration definieren die Adressen *Server IP Address* das hinter den Router angeschlossene Gerät. Bei Ping an die IP Adresse der SIM Karte antwortet der Router. Der Zutritt auf die Webschnittstelle des hinter den Router angeschlossenen Gerätes ist mit Port Forwarding möglich, bei dem der Außenanschluss, zu dem der Zutritt erwünscht wird, hinter die IP Adresse SIM angeführt wird. Beim Bedarf für den Anschluss 80 werden die einzelnen Außenanschlüsse (Public Port) geprüft, dort ist dieser Anschluss nicht definiert, darum wird bei der angekreuzten Option *Enable Remote HTTP Access* die Webschnittstelle des Routers automatisch geöffnet. Ist diese Option nicht angekreuzt und ist die Option *Send All Remaining Incoming Packets to Default Server* auc nicht angekreuzt, wird die Verbindung an die angeführte IP Adresse verwirklicht. Sind die Option der Webschnittstelle und die Default *Server IP Address* nicht angekreuzt, wird die Anforderung nicht durchgeführt.

Falls es erforderlich ist, mehr als 8 Regeln für NAT einzustellen, ist es möglich, folgendes Skript in Start-Up Script Window einzufügen:

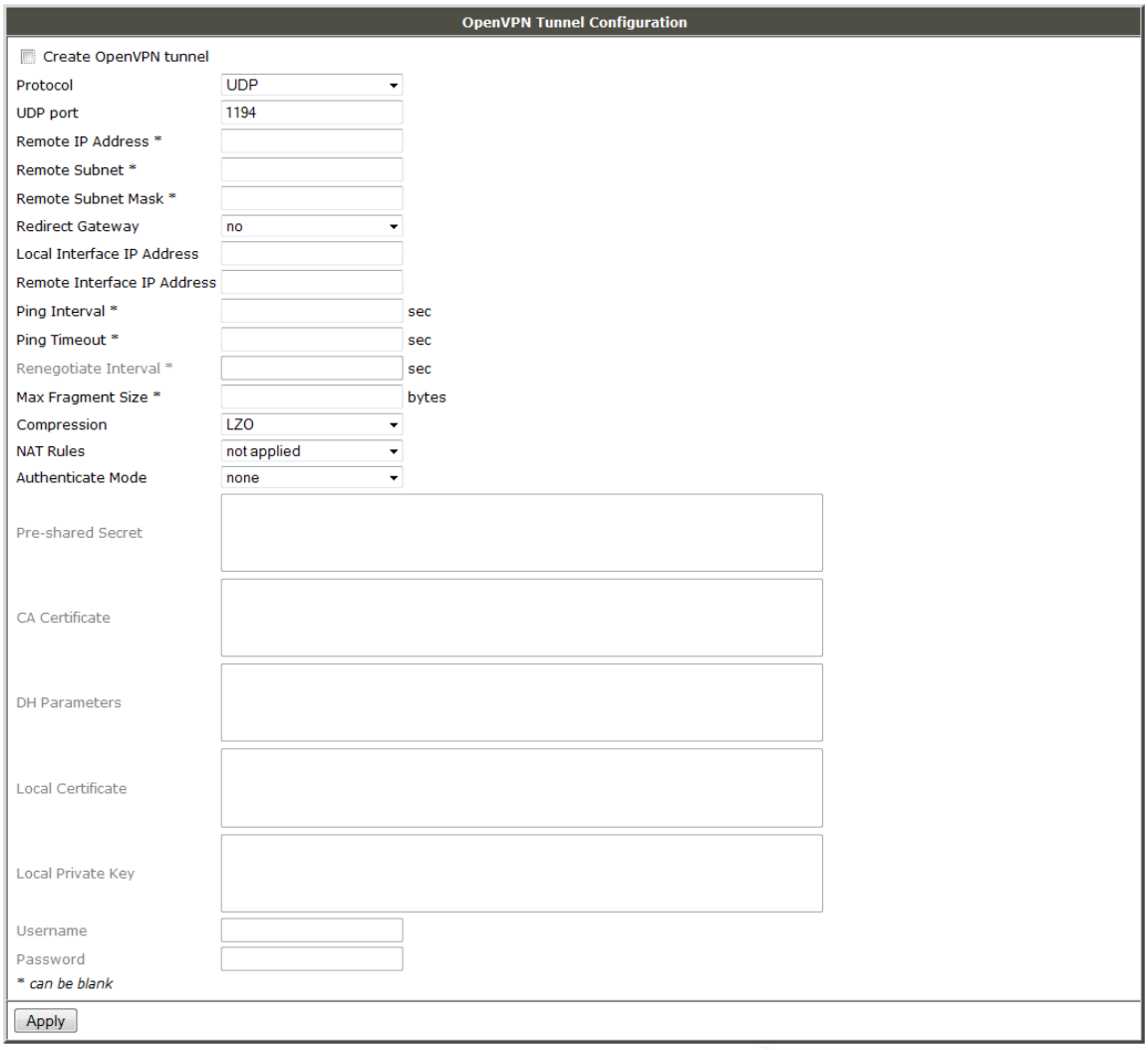
iptables -t nat -A napt -p tcp --dport [PORT_PUBLIC] -j DNAT --to-destination [IPADDR]:[PORT1_PRIVATE],

wo die sachlichen Anschlussnummern anstatt von [PORT_PUBLIC] und [PORT1_PRIVATE] einzufügen sind und IP Adresse anstatt von [IPADDR] einzufügen ist.

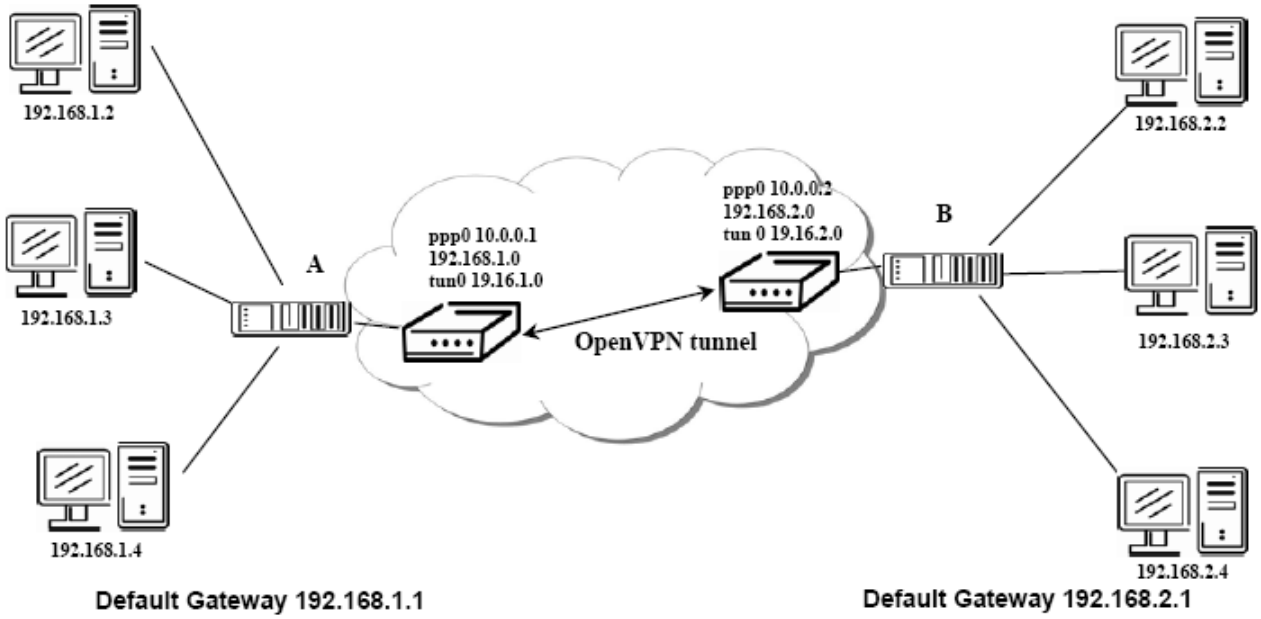
5.12. *Konfiguration des OpenVPN Tunnels*

Die Konfiguration des OpenVPN Tunnels kann durch die Auswahl der Option OpenVPN im Menü aufgerufen werden. Der OpenVPN Tunnel ermöglicht eine sichere (verschlüsselte) Verbindung von zwei LAN Netzen in ein Netz, das sich als homogen anstellt. Der OpenVPN Tunnel wird nach dem Ankreuzen der Option *Create OpenVPN Tunnel* aufgebaut.
Im Fenster kann das Protokoll *(Protocol)* definiert werden, mithilfe dessen OpenVPN die Kommunikation führt. Zur Auswahl steht das Protokoll *UDP*, *TCP Server* oder *TCP Client*, zu denen der Anschluss des Protokolls zugeteilt werden muss. Die Parameter definieren: *Remote IP Address* die IP Adresse der gegenüberliegenden Tunnelseite, *Remote Subnet* die Adresse vom Netz hinter der gegenüberliegenden Tunnelseite und *Remote Subnet Mask* die Maske vom Netz hinter der gegenüberliegenden Tunnelseite. Der Parameter *Redirect Gateway* ermöglicht den gesamten Verkehr im Ethernet umzulenken. Der Parameter *Local Interface IP Address* definiert die IP Adresse der lokalen Schnittstelle, der Parameter *Remote Interface IP Address* definiert die IP Adresse der Schnittstelle auf der gegenüberliegenden Tunnelseite. Der Parameter *Ping Interval* definiert das Zeitintervall, nach dessen Ablauf die Nachricht der gegenüberliegenden Seite gesendet wird und durch die Einstellung

des Parameters *Ping Timeout* wird eine von der gegenüberliegenden Seite gesandte Nachricht abgewartet. Zur richtigen Verifizierung des OpenVPN Tunnels muss der Parameter *Ping Timeout* größer als *Ping Interval* sein. Der Parameter *Renegotiate Interval* stellt die Periode der erneuten Negotiation (der erneuten Autorisierung) des OpenVPN Tunnels ein. Dieser Parameter kann nur bei der Verifizierung des User Names/Passwords oder bei Verwendung des Zertifikats X.509 eingestellt werden. Mit dem Parameter *Max Fragment Size* ist es möglich, die maximale Größe des abgesandten Pakets zu definieren. Die abgesandten Daten können mit verlustfreier LZO Komprimierung im Parameter *Compression* verdichtet werden, die Komprimierung muss an beiden Tunnelseiten eingestellt werden. Im Parameter *NAT Rules* können die eingestellten NAT Regeln auf den OpenVPN Tunnel angewandt werden oder diese Anwendung muss nicht erfolgen. Mit dem Parameter *Authenticate Mode* ist es möglich, die Authentisierung einzustellen. Zur Auswahl stehen auch: keine Authentisierung (None), oder Authentisierung mittels *Pre-shared Secret*, mit diesem Parameter wird ein geteilter Schlüssel für beide Tunnelseiten eingestellt; oder *User Name / Password*, dieser Parameter ermöglicht die Authentisierung mittels *CA Certificate*, *User Name* und *Password*; oder *X.509 Certificate (Client)*, der Parameter ermöglicht die Authentisierung mittels *CA Certificate*, *Local Certificate* und *Local Private Key*; oder aber *X.509 Certificate (Server)*, der Parameter ermöglicht die Authentisierung mittels *CA Certificate, DH Parameters, Local Certificate* und *Local Private Key*.



Beispiel für die Konfiguration des OpenVPN Tunnels:

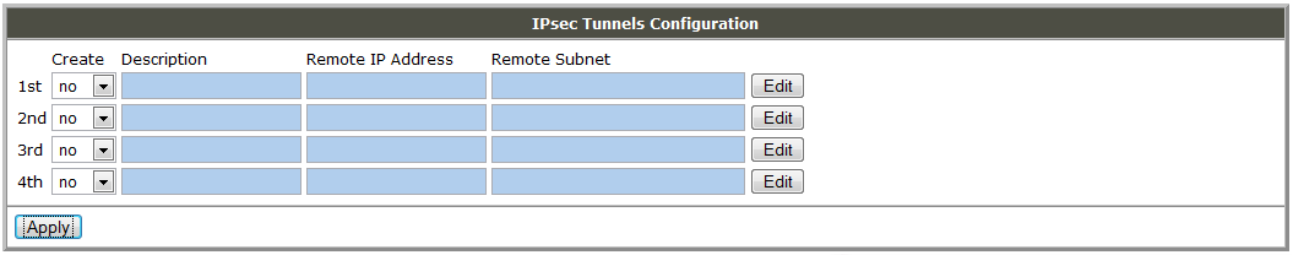


Konfiguration des OpenVPN Tunnels:

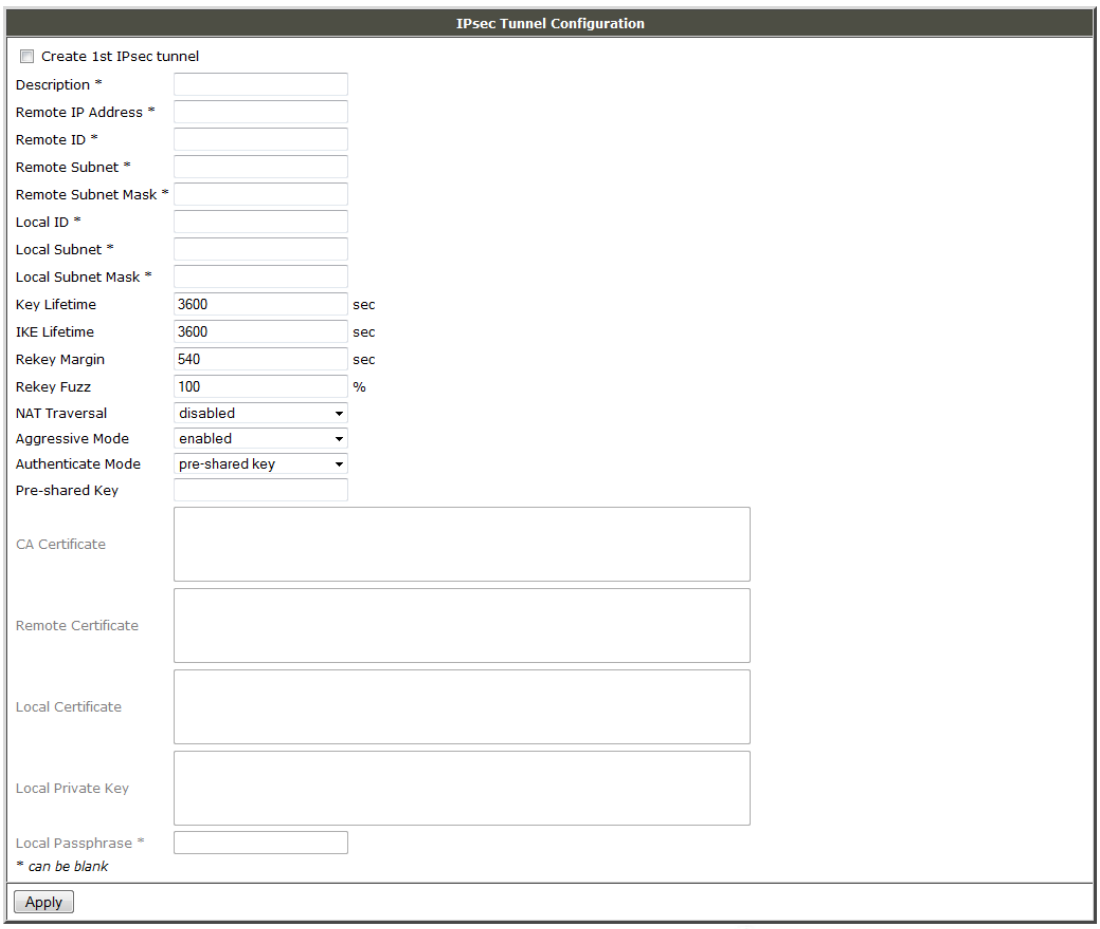
	A	B
Protocol	UDP	UDP
UDP Port	1194	1194
Remote IP Address:	10.0.0.2	10.0.0.1
Remote Subnet:	192.168.2.0	192.168.1.0
Remote Subnet Mask:	255.255.255.0	255.255.255.0
Local Interface IP Address:	19.16.1.0	19.16.2.0
Remote Interface IP Address:	19.16.2.0	19.16.1.0
Compression	LZO	LZO
Authenticate mode:	none	none

5.13. *Konfiguration des IPSec Tunnels*

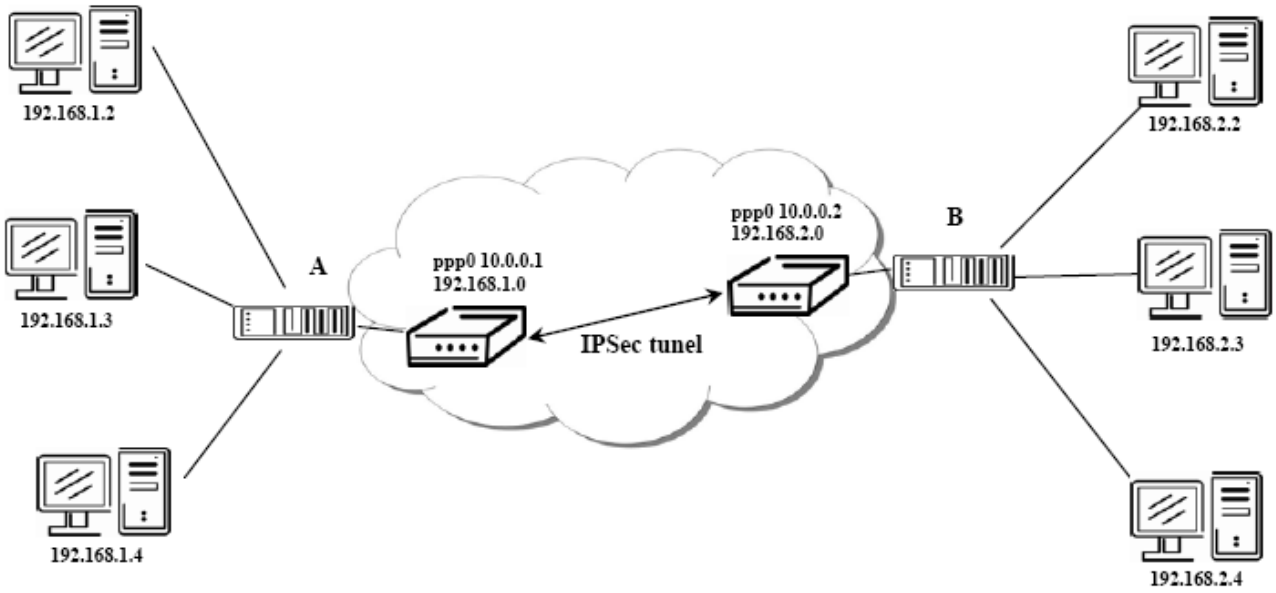
Der IPsec Tunnel erzeugt eine sichere (verschlüsselte) Verbindung von zwei LAN Netzen in ein Netz, das sich als homogen anstellt. Der Router bietet die Möglichkeit bis zu vier IPsec Tunnel zu erzeugen, deren Konfiguration durch die Auswahl der Option *IPsec* im Menü aufgerufen werden kann. Im Fenster *IPsec Tunnels Configuration* sind vier Zeilen, jede Zeile entspricht der Konfiguration von jeweils einem Tunnel. Die Spalte *Create* schaltet die einzelnen Tunnel ein, die anderen Spalten beinhalten die Ansicht der im Fenster *IPsec Tunnel Configuration* eingestellten Werte, dieses Fenster wird durch die Betätigung der Taste *Edit* angezeigt.



Im Fenster *IPsec Tunnel Configuration* können die Tunnelbezeichnung *(Description)*, die IP Adresse der gegenüberliegenden Tunnelseite *(Remote IP Address)*, die ID der gegenüberliegenden Seite *(Remote ID)*, die Adresse vom Netz hinter der gegenüberliegenden Tunnelseite *(Remote Subnet)*, die Maske vom Netz hinter der gegenüberliegenden Tunnelseite *(Remote Subnet Mask)*, die ID der lokalen Seite *(Local ID)*, die Adresse vom Lokalnetz *(Local Subnet)*, die Maske vom Lokalnetz *(Local Subnet Mask)*, die Lebensdauer vom Schlüssel *(Key Lifetime)* und die Lebensdauer von IKA SA *(IKE lifetime)* definiert werden. Der Parameter *Rekey Margin* bestimmt die Zeit vor dem Ablauf der Gültigkeit der Schlüssel, wenn neue Schlüssel erzeugt werden. Darüber hinaus wird diese Zeit bis um *Rekey Fuzz* Prozente vom Wert des Parameters Rekey Margin zufälligerweise verlängert. Wird die Adressenübersetzung zwischen zwei Endpunkten des IPsec Tunnels benutzt, ist es notwendig NAT *Traversal (Enabled)* freizugeben. Durch das Ankreuzen des Parameters *Aggressive Mode* wird der angreifende Modus beim Verbindungsaufbau eingestellt. Die Verbindung wird dann schneller aufgebaut, aber die Verschlüsselung wird auf 3DES-MD5 fest eingestellt. Die Authentisierung kann mit dem Parameter *Authenticate mode* eingestellt werden, zur Auswahl stehen die Möglichkeiten *Pre-shared Key oder* Zertifikat X.509. MIt dem Parameter *Pre-shared Key* wird dann der geteilte Schlüssel für beide Tunnelseiten eingestellt. Bei der Authentisierung mit dem Zertifikat X.509 sind die Zertifikate *CA Certificate, Remote Certificate, Local Certificate, Privatschlüssel Local Private Key* und *Local Passphrase* einzufügen. Die Zertifikate und der Privatschlüssel müssen im Format PEM sein. Als Zertifikat kann nur ein solches Zertifikat benutzt werden, das mit Anfang und Ende des Zertifikats eingeleitet wird. Die Parameter ID setzen sich aus zwei Teilen, *Host Name* und *Domain Name*, zusammen. Die Optionen, die leer sein können, werden zur genauen Identifizierung vom IPsec Tunnel benutzt.
Die Änderungen der Einstellungen wirken sich nach der Betätigung der Apply Taste aus.



Beispiel für die Konfiguration des IPSec Tunnels:

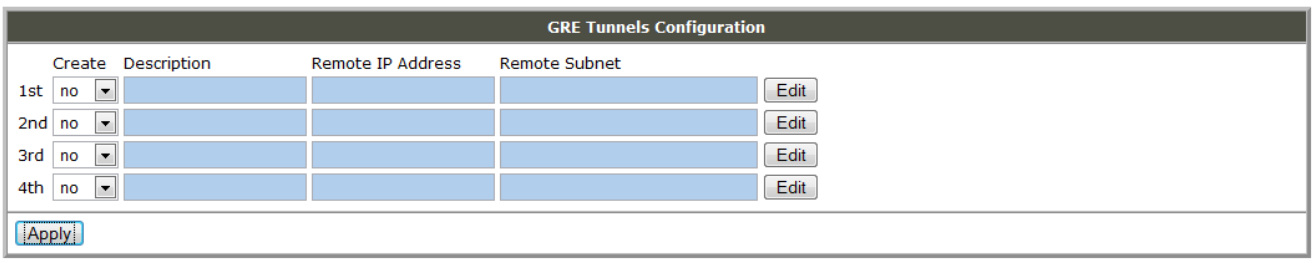


Konfiguration des IPSec Tunnels:

	A	B
Remote IP Address:	10.0.0.2	10.0.0.1
Remote Subnet:	192.168.2.0	192.168.1.0
Remote Subnet Mask:	255.255.255.0	255.255.255.0
Local Subnet:	192.168.1.0	192.168.2.0
Local Subnet Mask:	255.255.255.0	255.255.255.0
Authenticate mode:	pre-shared key	pre-shared key
Pre-shared key	test	test

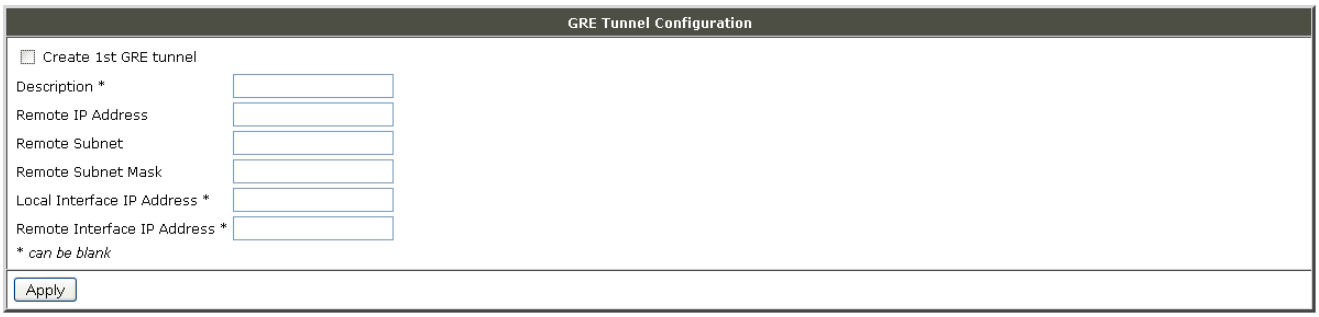
5.14. *Konfiguration des GRE Tunnels*

Der GRE Tunnel erzeugt eine Verbindung von zwei LAN Netzen in ein Netz, das sich als homogen anstellt. Der Router bietet die Möglichkeit, bis zu vier GRE Tunnel zu erzeugen, deren Konfiguration durch die Auswahl der Option *GRE* im Menü aufgerufen werden kann. Im Fenster *GRE Tunnels Configuration* sind vier Zeilen, jede Zeile entspricht der Konfiguration von jeweils einem Tunnel. Die Spalte *Create* schaltet die einzelnen Tunnel ein, die anderen Spalten beinhalten die Ansicht der im Fenster *GRE Tunnel Configuration* eingestellten Werte, dieses Fenster wird durch Betätigung der Taste *Edit* angezeigt.

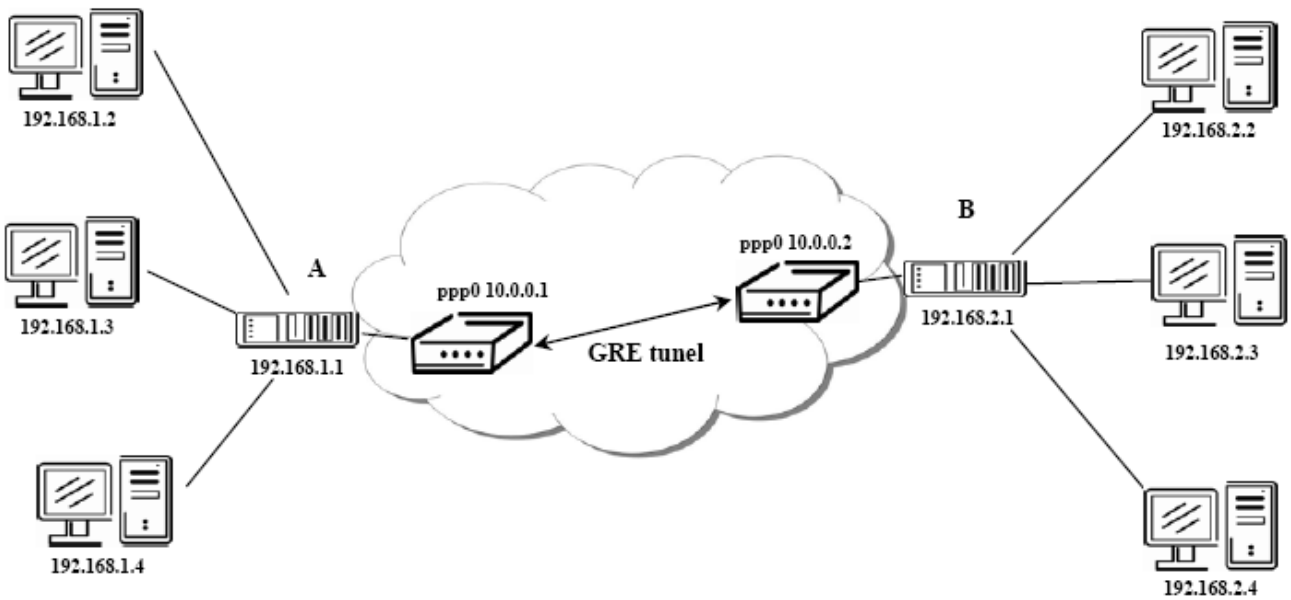


Die Tunnel werden durch das Ankreuzen der Option *Create x GRE Tunnel* aktiviert. Weiter können die Bezeichnung des GRE Tunnels *(Description)*, die IP Adresse der gegenüberliegenden Tunnelseite *(Remote IP Address)*, die interne IP Adresse des Tunnels auf der lokalen Tunnelseite *(Local Interface IP Address)*, die interne IP Adresse der gegenüberliegenden Tunnelseite *(Remote Interface IP Address)*, die Adresse vom Netz hinter der gegenüberliegenden Tunnelseite *(Remote Subnet)* und die Maske vom Netz hinter der gegenüberliegenden Tunnelseite *(Remote Subnet Mask)* definiert werden.

Vorsicht, der GRE Tunnel kommt an der Übersetzung der NAT Adressen nicht weiter.
Die Änderungen der Einstellungen wirken sich nach der Betätigung der Apply Taste aus.



Beispiel für die Konfiguration des GRE Tunnels:

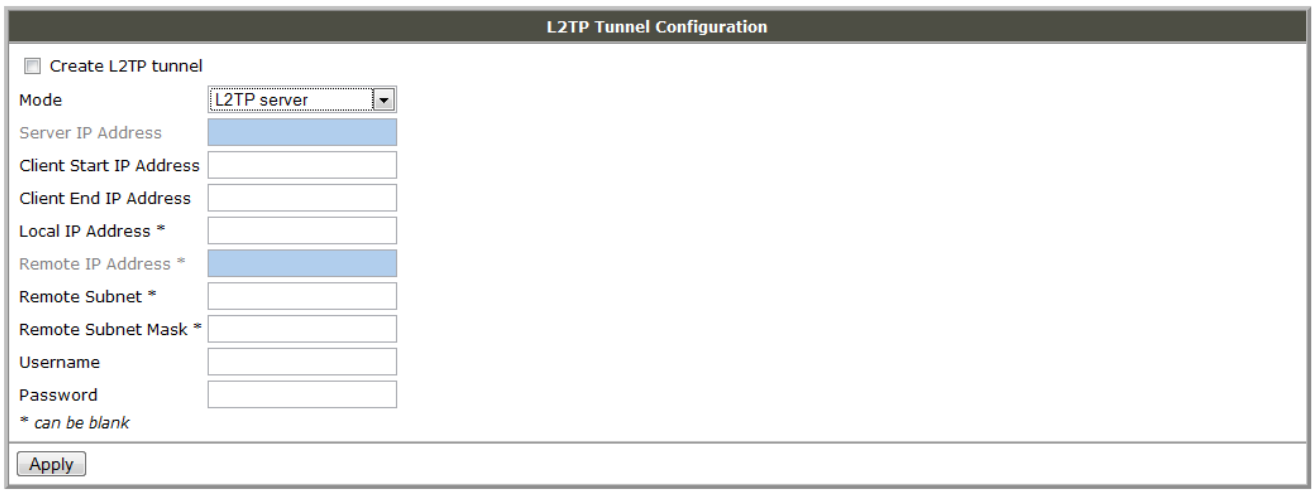


Konfiguration des GRE Tunnels:

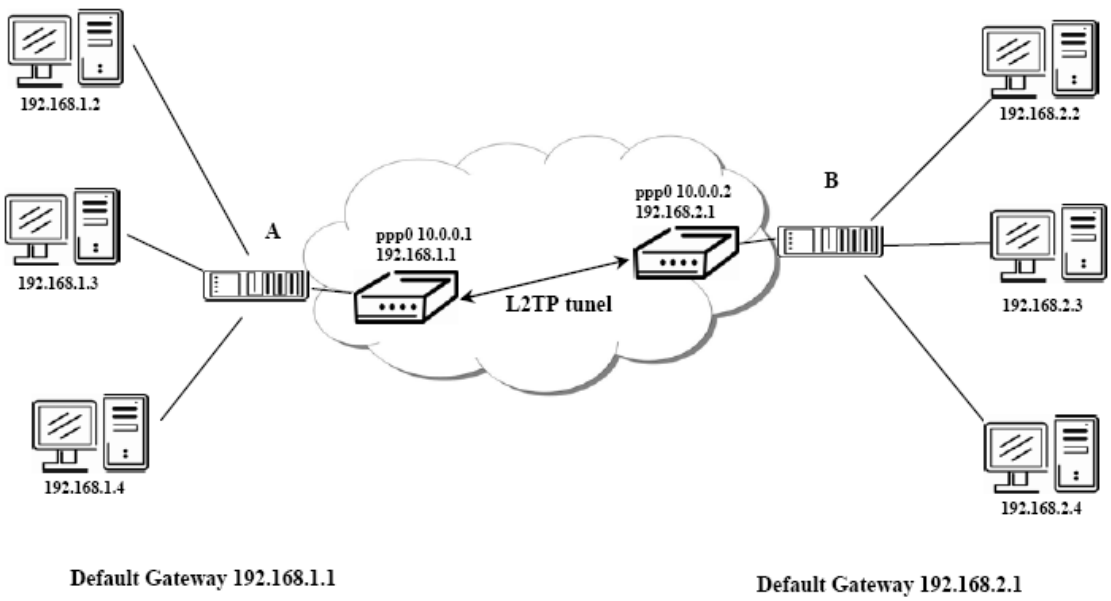
	A	B
Remote External IP Address:	10.0.0.2	10.0.0.1
Remote Subnet:	192.168.2.0	192.168.1.0
Remote Subnet Mask:	255.255.255.0	255.255.255.0

5.15. *Konfiguration des L2TP Tunnels*

Die Konfiguration des L2TP Tunnels kann durch die Auswahl der Option L2TP im Menü aufgerufen werden. Der L2TP Tunnel wird zur Verbindung von zwei LAN Netzen in ein Netz mit Authentisierung benutzt, wobei sich das Netz als homogen anstellt. Der L2TP Tunnel wird nach dem Ankreuzen der Option *Create L2TP Tunnel* aufgebaut.
Im Fenster können der Modus *(Mode)* des L2TP Tunnels auf der Routerseite, die IP Serveradresse *(Server IP Address)* bei Kunden, die vom Server den Klienten angebotene IP Anfangsadresse *(Client Start IP Address)*, die vom Server den Klienten angebotene IP Endadresse *(Client End IP Address)*, die IP Adresse des Tunnels auf der lokalen Seite *(Local IP Address)*, die IP Adresse der gegenüberliegenden Tunnelseite *(Remote IP Address)*, die Adresse vom Netz hinter der gegenüberliegenden Tunnelseite *(Remote Subnet)*, die Maske vom Netz hinter der gegenüberliegenden Tunnelseite *(Remote Subnet Mask)*, der Anmeldungsname zur Anmeldung in den L2TP Tunnel *(User Name)* und das Passwort *(Password)* definiert werden.
Die Änderungen der Einstellungen wirken sich nach der Betätigung der Apply Taste aus.



Beispiel für die Konfiguration des L2TP Tunnels:

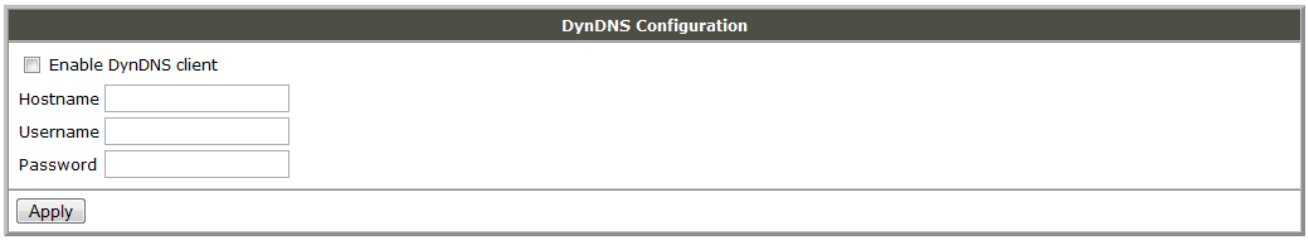


Konfiguration des L2TP Tunnels:

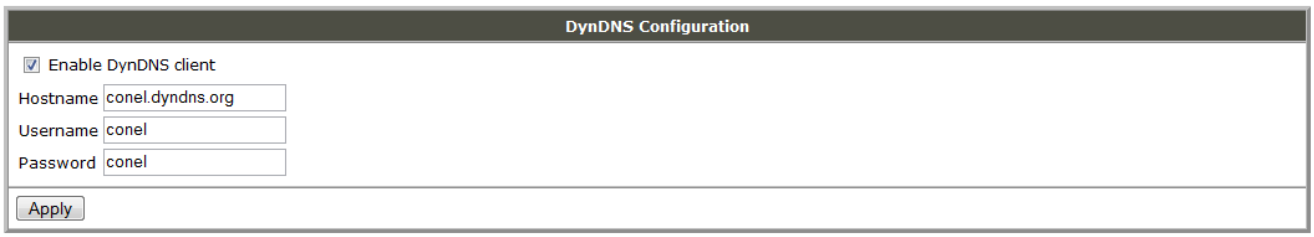
	A	B
Mode	L2TP Server	L2TP Client
Server IP Address	---	10.0.0.1
Client Start IP Address:	192.168.3.2	---
Client End IP Address:	192.168.3.254	---
Local IP Address:	192.168.3.1	---
Remote IP Address	---	---
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

5.16. *Konfiguration des DynDNS Klienten*

Die Konfiguration des DynDNS Klienten kann durch die Auswahl der Option DynDNS im Menü aufgerufen werden. Im Fenster können die am Server www.dyndns.org registrierte Domäne der dritten Größenordnung *(Hostname)*, der Anmeldungsname *(User Name)* und Passwort *(Password)* definiert werden.
Die Änderungen der Einstellungen wirken sich nach der Betätigung der Apply Taste aus.



Beispiel für die Konfiguration des DynDNS Klienten mit der Domäne conel.dyndns.org, dem Benutzernamen conel und Passwort conel:



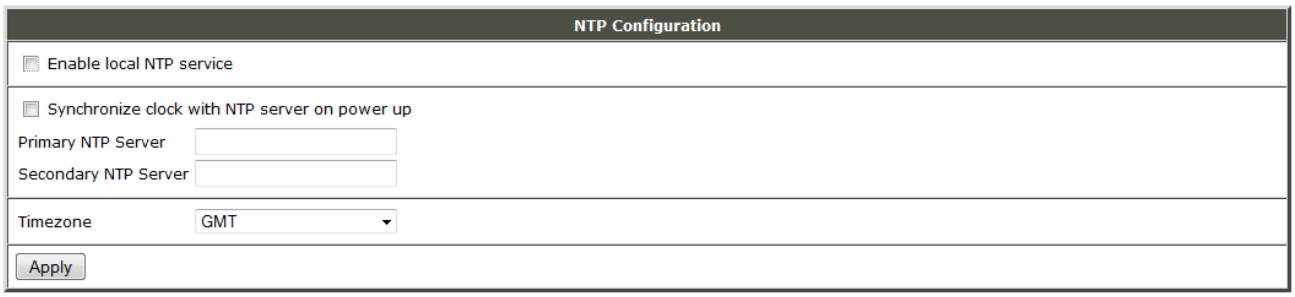
Teilt der Netzbetreiber die DNS Server nicht zu, ist es möglich die Server durch das Einfügen vom Skript im Start-Up Script Window zu konfigurieren:

echo “nameserver xxx.xxx.xxx.xxx“ > /etc/resolf.conf, wo xxx.xxx.xxx.xxx die IP Adresse des ersten DNS Servers ist,

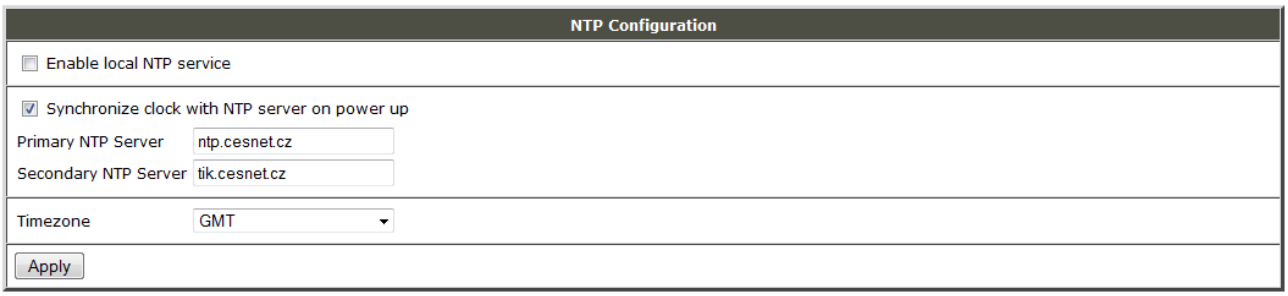
echo “nameserver yyy.yyy.yyy.yyy“ >> /etc/resolf.conf, wo yyy.yyy.yyy.yyy die IP Adresse des zweiten DNS Servers ist.

5.17. *Konfiguration des NTP Klienten*

Die Konfiguration des NTP Klienten kann durch die Auswahl der Option NTP im Menü aufgerufen werden. Im Fenster können die Adressen des primären *(Primary NTP Server Address)* und des sekundären NTP Servers *(Secondary NTP Server Address)* definiert werden, mittels der der Router nach dem ersten Verbindungsaufbau in GPRS ab der Einschaltung der Stromversorgung die interne Uhr stellt. Beispiel für die Adresse des NTP Servers kann ntp.cesnet.cz und tik.cesnet.cz sein. Mit dem Parameter *Timezone* kann die Zeitzone des Routers eingestellt werden.
Der Parameter *Enable Local NTP Service* stellt den Router in den Modus, bei dem er als NTP Server für andere Geräte funktioniert.
die Änderungen der Einstellungen wirken sich nach der Betätigung der Apply Taste aus.

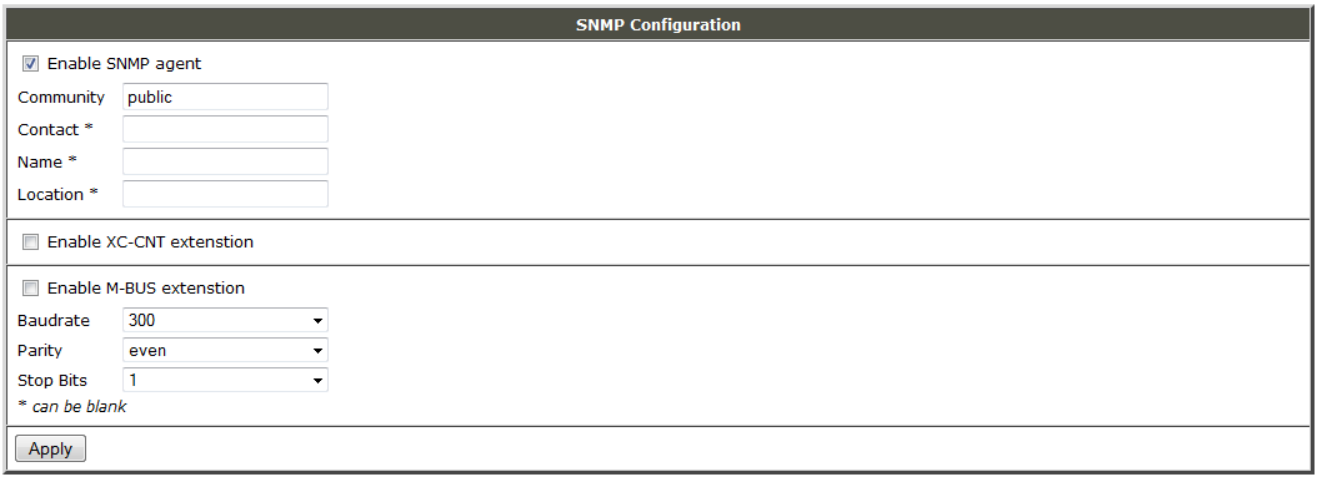


Beispiel für die NTP Konfiguration mit dem eingestellten primären und sekundären NTP Server.



5.18. *Konfiguration des SNMP Agenten*

Durch das Aufrufen der Option SNMP ist die Konfiguration des SNMP Agenten Ver.1 möglich, der die Informationen über den Router bzw. über den Zustand des Erweiterungsanschlusses CNT oder MBUS sendet.
Die Option *Community* definiert das Passwort zum Zutritt zum SNMP Agenten. Die Option *Contact* identifiziert die Person, die den Router verwaltet, zusammen mit den Informationen, wie der Kontakt mit dieser Person aufzunehmen ist. Die Option *Name* ist die Benennung des Routers und die Option *Location* beschreibt die tatsächliche Unterbringung des Routers.
Durch das Ankreuzen der Option *Enable XC-CNT* extension ist es möglich, den Zustand der Eingänge am Erweiterungsanschluss CNT zu überwachen, oder durch Ankreuzen der Option *Enable M-BUS extension* und durch Einstellung der Geschwindigkeit der Kommunikation *(Baudrate)*, der Parität *(Parity)* und der Anzahl von Stoppbits *(Stop Bits)* ist es möglich, den Zustand der angeschlossenen Messgeräte am Erweiterungsanschluss MBUS zu überwachen. Diese zwei Parameter können nicht gleichzeitig angekreuzt werden.



Jeder überwachte Wert ist mittels des numerischen Identifikators **OID** – *Object Identifier* eindeutig identifiziert. OID endet mit „.9“.
Für den Erweiterungsanschluss CNT wird der folgende OID Bereich (der internen Variablen) verwendet:

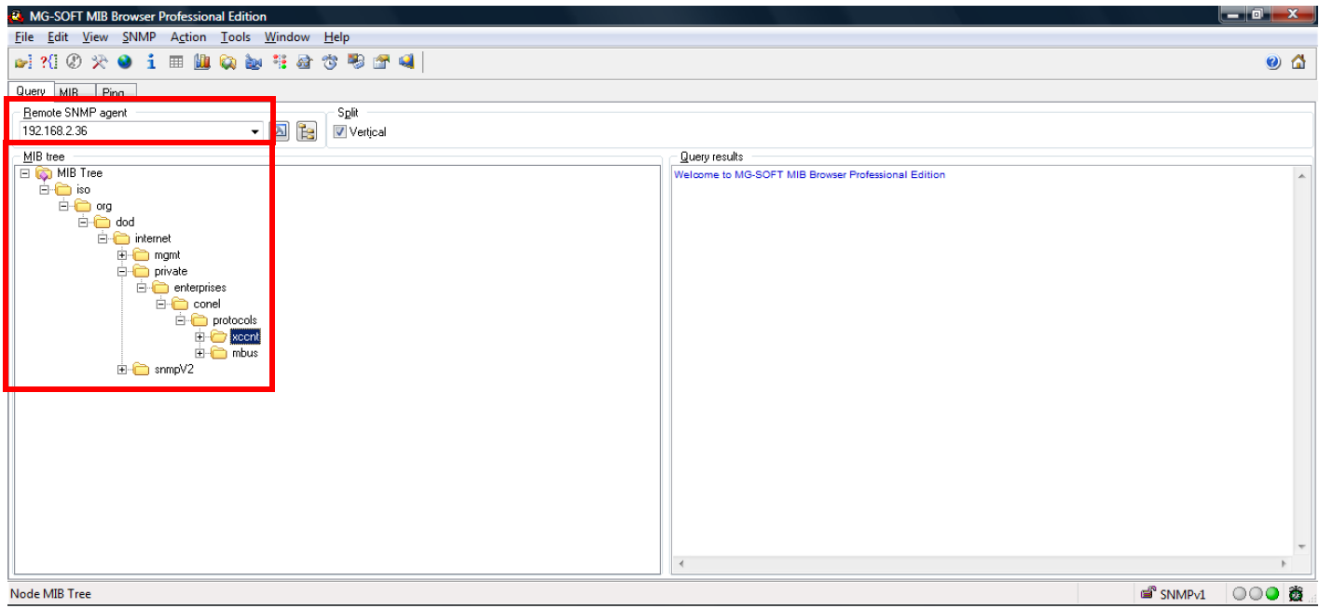
OID	Bedeutung
.1.3.6.1.4.1.30140.2.1.1.0	Analogeingang AN1 (Bereich 0-4095)
.1.3.6.1.4.1.30140.2.1.2.0	Analogeingang AN2 (Bereich 0-4095)
.1.3.6.1.4.1.30140.2.1.3.0	Zählereingang CNT1 (Bereich 0-4294967295)
.1.3.6.1.4.1.30140.2.1.4.0	Zählereingang CNT2 (Bereich 0-4294967295)
.1.3.6.1.4.1.30140.2.1.5.0	Binäreingang BIN1 (Werte 0,1)
.1.3.6.1.4.1.30140.2.1.6.0	Binäreingang BIN2 (Werte 0,1)
.1.3.6.1.4.1.30140.2.1.7.0	Binäreingang BIN3 (Werte 0,1)
.1.3.6.1.4.1.30140.2.1.8.0	Binäreingang BIN4 (Werte 0,1)

Für den Erweiterungsanschluss MBUS wird der folgende OID Bereich (der internen Variablen) verwendet:

OID	Bedeutung
.1.3.6.1.4.1.30140.2.2.<address>.1.0	IdNumber – Nummer des Messgeräts
.1.3.6.1.4.1.30140.2.2.<address>.2.0	Manufacturer – Hersteller
.1.3.6.1.4.1.30140.2.2.<address>.3.0	Version – spezifiziert die Version des Messgeräts
.1.3.6.1.4.1.30140.2.2.<address>.4.0	Medium – Typ des gemessenen Mediums
.1.3.6.1.4.1.30140.2.2.<address>.5.0	Status – Meldungen der Fehlerzustände
.1.3.6.1.4.1.30140.2.2.<address>.6.0	0. VIF – Informationsfeld mit Wert
.1.3.6.1.4.1.30140.2.2.<address>.7.0	0. gemessener Wert
.1.3.6.1.4.1.30140.2.2.<address>.8.0	1. VIF – Informationsfeld mit Wert
.1.3.6.1.4.1.30140.2.2.<address>.9.0	1. gemessener Wert
.1.3.6.1.4.1.30140.2.2.<address>.100.0	47. VIF – Informationsfeld mit Wert
.1.3.6.1.4.1.30140.2.2.<address>.101.0	47. gemessener Wert

Die Anschrift des Messgerätes kann aus dem Bereich 0. bis 254 sein, wobei 254 Broadcast ist.

Beispiel für einen MIB Browser:



Es ist wichtig die IP Adresse vom SNMP Agenten (Router) im Feld *Remote SNMP agent* einzustellen. Nach der Eingabe der IP Adresse ist es im Teil *MIB tree* möglich die internen Variablen anzuzeigen. Der Pfad zu den Variablen ist:
iso->org->dod->internet->private->enterprises->conel->protocols

5.19. *Konfiguration und Versenden von SMS*

Die SMS Konfiguration wird durch die Auswahl der Option *SMS* im Hauptmenü aufgerufen. Im ersten Fensterteil wird das Versenden der SMS konfiguriert. In der Konfiguration des SMS Versandes ist es möglich, das automatische Versenden einer SMS nach dem Einschalten der Stromversorgung *(Send SMS on Power Up)*, beim Verbindungsaufbau *(Send SMS on PPP Connect)* oder beim Verlust der PPP Verbindung *(Send SMS on PPP Disconnect)* sowie bei Überschreitung des Datengrenzwerts *(Send SMS When Data Limit Exceeded)* einzustellen. Der Parameter *Send SMS When Binary Input Is Active* stellt das Versenden der SMS beim aktiven Binärausgang sicher, wobei der Text der SMS-Nachricht mit den Parametern BIN1-SMS bis BIN4-SMS festgelegt wird. Die Information wird bis auf drei Telefonnummern versendet. Das Feld *Unit ID* ist die Benennung des Routers, die gegebenenfalls in der SMS abgesandt wird, diese Benennung kann ein beliebiges Format haben.

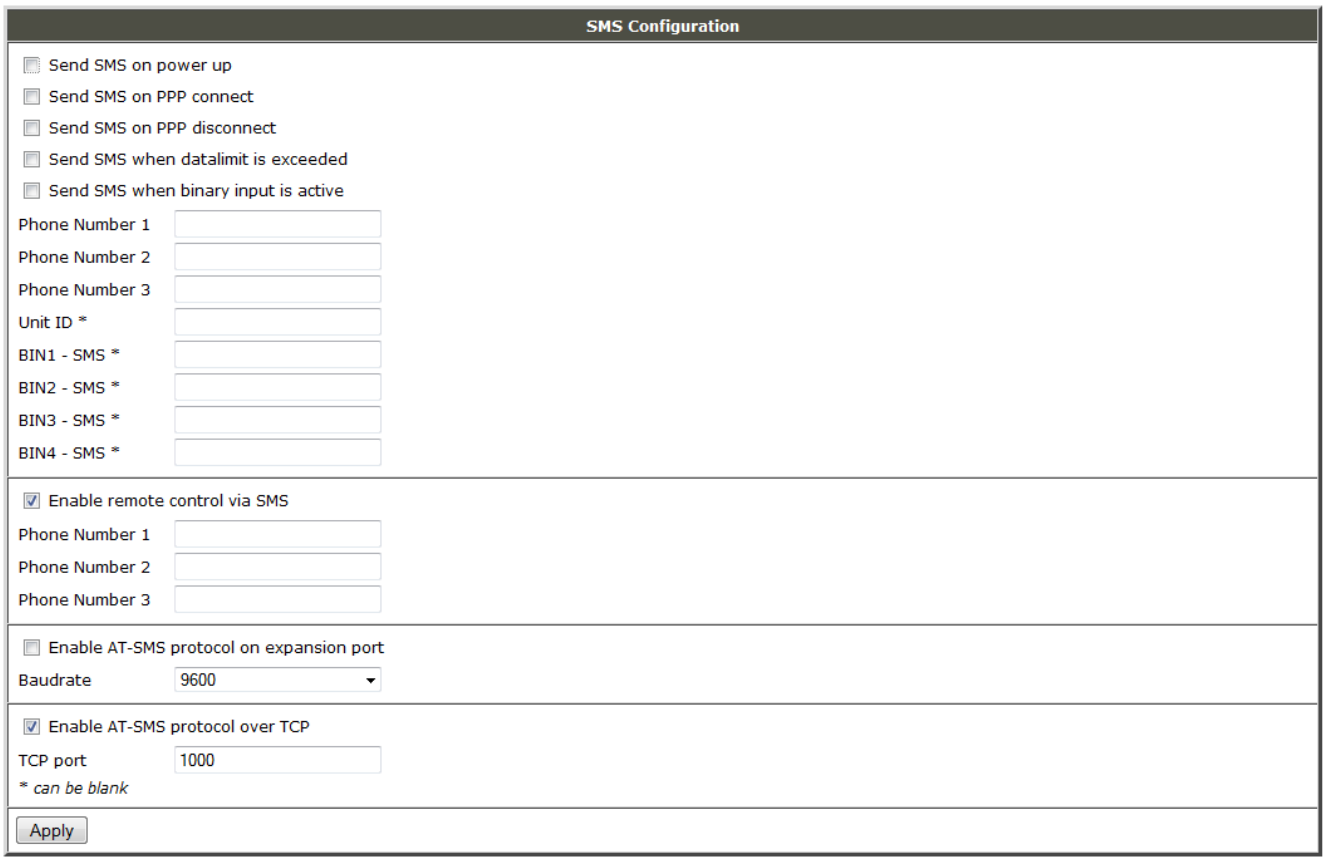
Im zweiten Teil ist es möglich, die Betätigung des Routers mittels SMS Nachrichten zu konfigurieren. Nach dem Ankreuzen der Option *Enable remote control* via SMS ist es möglich, die PPP Verbindung mittels einer SMS Nachricht aufzubauen oder abzuschließen. Diese Betätigung kann für bis zu drei Telefonnummern eingestellt werden. Ist die Betätigung des Routers mittels SMS Nachrichten eingestellt, werden alle ankommenden SMS automatisch bearbeitet und gelöscht. In der Ausgangseinstellung ist dieser Parameter eingeschaltet.

Ist keine Telefonnummer ausgefüllt, ist es möglich den Router erneut zu starten, und zwar durch das Versenden der SMS Nachricht im Format *Reboot* von einer beliebigen Nummer aus. Sind eine oder mehrere Nummern ausgefüllt, ist es möglich, den Router mittels der nur von diesen Nummern gesandten SMS Nachrichten zu betätigen.

Es sind SMS im Format möglich:

SMS	Bedeutung
go online sim 1	Umschaltung auf erste SIM (APN1)
go online sim 2	Umschaltung auf zweite SIM (APN2)
go online	Der Router wird in den Modus Online umgeschaltet
go offline	Beendigung der PPP Verbindung
set out=0	Der Ausgang vom Anschluss CNT wird auf 0 gesetzt
set out=1	Der Ausgang vom Anschluss CNT wird auf 1 gesetzt
reboot	Neustart des Routers

Durch die Auswahl der Option *Enable AT-SMS Protocol on External Port* und durch die Einstellung der Geschwindigkeit *(Baudrate)* ist es möglich, das Versenden / den Empfang von SMS Nachrichten am seriellen Anschluss freizugeben.
Durch die Auswahl der Option *Enable AT-SMS Protocol on TCP Port* ist es möglich, das Versenden / den Empfang von SMS Nachrichten am TCP Anschluss freizugeben. Die SMS Nachrichten werden mittels der standardmäßigen AT Befehle versandt. Mehr über AT finden Sie in [1].
Die Optionen *Enable AT-SMS Protocol on External Port* und *Enable AT-SMS Protocol on TCP Port* dürfen nicht gleichzeitig angekreuzt werden.



Nach dem Einschalten der Stromversorgung (Power Up) kommen an die angeführten Telefonnummern die SMS im Format an:

UR5 (Unit ID) has been powered up. GSM signal strenght: -xx dBm. wobei GSM signal strenght – Signalpegel bedeutet

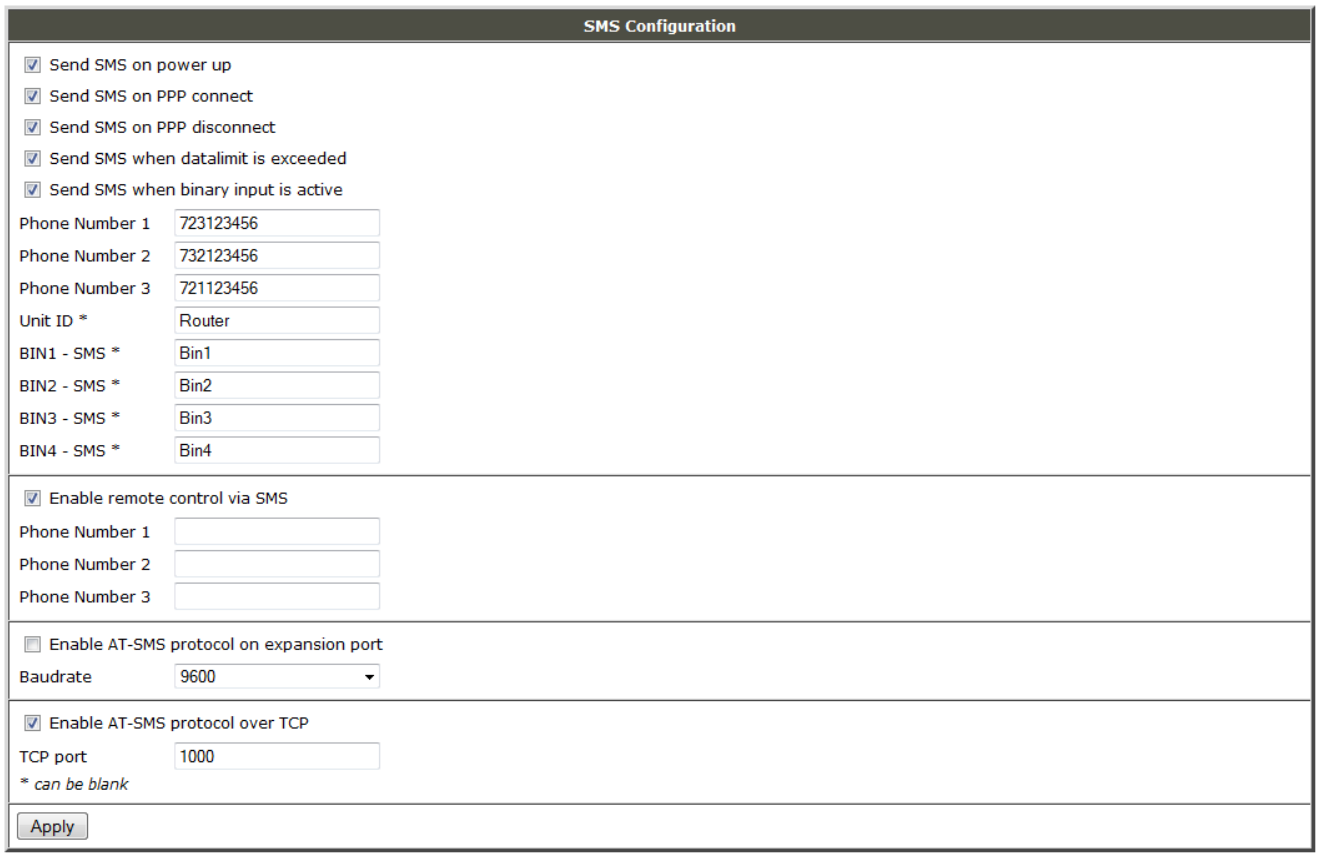
Nach dem Aufbau der PPP Verbindung (PPP Connect) kommen an die angeführten Telefonnummern die SMS im Format an:

UR5 (Unit ID) has established PPP connection.

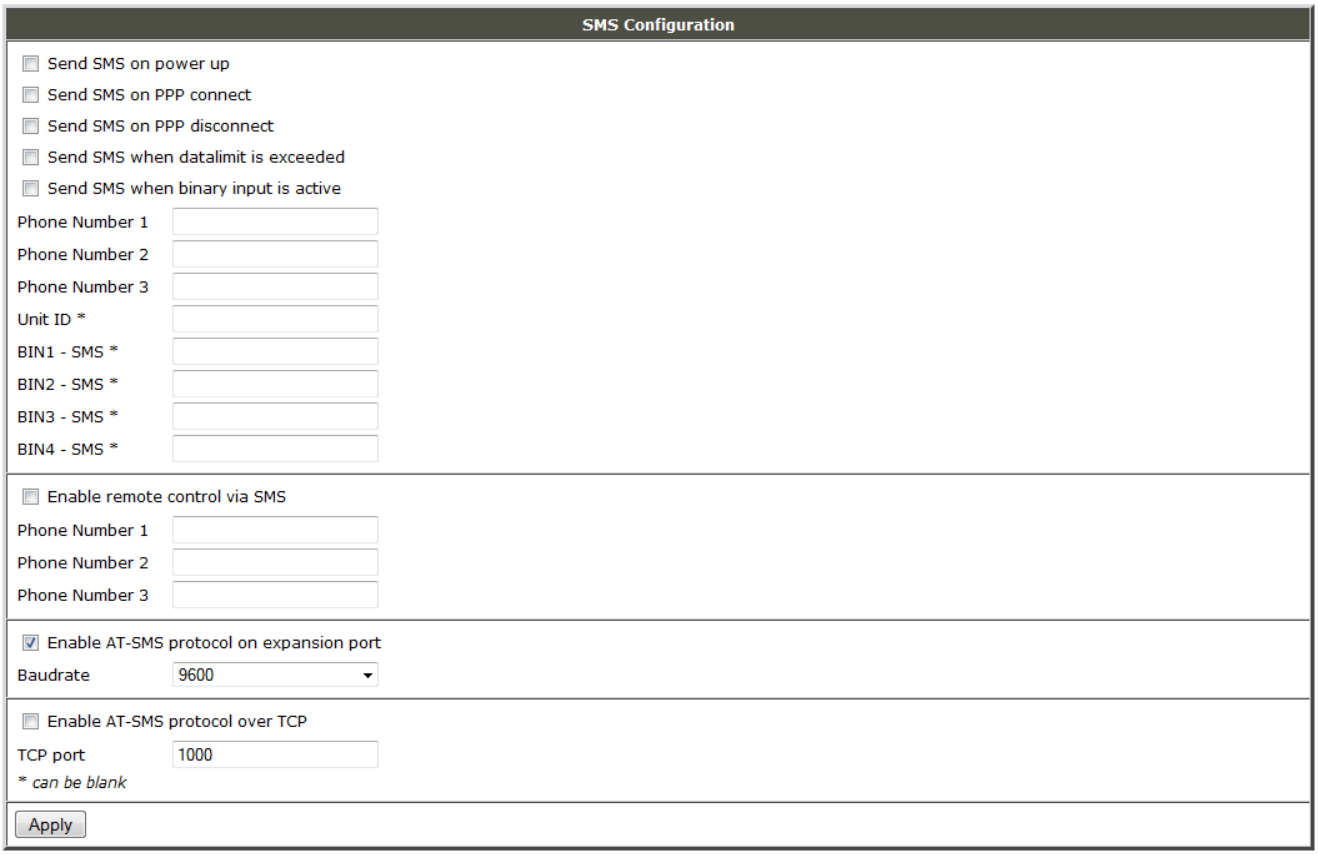
Nach dem Verlust der PPP Verbindung (PPP Disconnect) kommen an die angeführten Telefonnummern die SMS im Format an:

UR5 (Unit ID) has lost PPP connection.

Die Einstellung des Versendens von diesen SMS lautet wie folgt:



Beispiel für die UR5 Routereinstellung zum Versand von SMS Nachrichten über die serielle Schnittstelle:



Mit den SMS Nachrichten ist es möglich, z. B. im Programm Hyperterminal zu arbeiten. Nach dem Aufbau der Verbindung mit dem UR5 Router über die serielle Schnittstelle oder Ethernet ist es möglich mittels der folgenden AT Befehle mit den SMS Nachrichten zu arbeiten (mehr AT Befehle in der Literatur [1]):

AT commands	Description
AT+CMGF=1	Set the text mode for SMS writing
AT+CMGS=”tel. number”	Commands enables to send SMS on entered tel. number
AT+CMGL=ALL	List of all SMS messages
AT+CMGR=<index>	Read of the definite SMS (all SMS has our index)
AT+CMGD=<index>	SMS delete according to index

Zum Einstellen des Schreibens einer SMS Nachricht im Textmodus wird der Befehl *AT+CMGF=1* angewandt.
AT+CMGF=1 Enter
OK
Die Textnachricht wird mittels des Befehls *AT+CMGS=<Telefonnummer>* erstellt. Nach der Betätigung der *Enter* Taste wird das Zeichen > angezeigt, dahinter kann der eigene Text der SMS Nachricht geschrieben werden. Nach dem Verfassen der SMS wird die Tastenkombination *CTRL+Z* zum Versenden verwendet (das Versenden der SMS Nachricht dauert einige Zeit). Das Verfassen der Nachricht wird mit der Taste Esc aufgehoben.

AT+CMGS=“712123456“ Enter
>***Hello World!*** CTRL+Z (Tastenkombination)
OK

Mit dem Befehl *AT+CMGL=ALL* ist es möglich, eine neue SMS zu ermitteln. Mit diesem Befehl werden alle SMS Nachrichten eingelesen.

AT+CMGL=ALL Enter
+CMGL: <Index>, <Status>,<Absendernummer>, <Datum>,<Zeit>
Text der SMS Nachricht.
+CMGL: 1,“REC UNREAD“,“+420721123456“, ,“08/02/02, 10:33:26+04“
Hello World!
wo <Index> die laufende Nummer der SMS Nachricht ist,
<Status> der Zustand der SMS Nachricht ist:
REC UNREAD – SMS Nachricht nicht gelesen
REC READ – SMS Nachricht gelesen
STO UNSENT – gespeicherte, nicht abgesandte SMS Nachricht
STO SENT – gespeicherte, abgesandte SMS Nachricht
ALL – alle SMS Nachrichten
<Absendernummer> ist die Telefonnummer, von der die SMS Nachricht empfangen wurde,
<Datum> das Datum des SMS Empfangs lautet,
<Zeit> die Zeit des SMS Empfangs lautet.

Die neue SMS Nachricht kann mit dem Befehl AT+CMGR=<Index> gelesen werden.

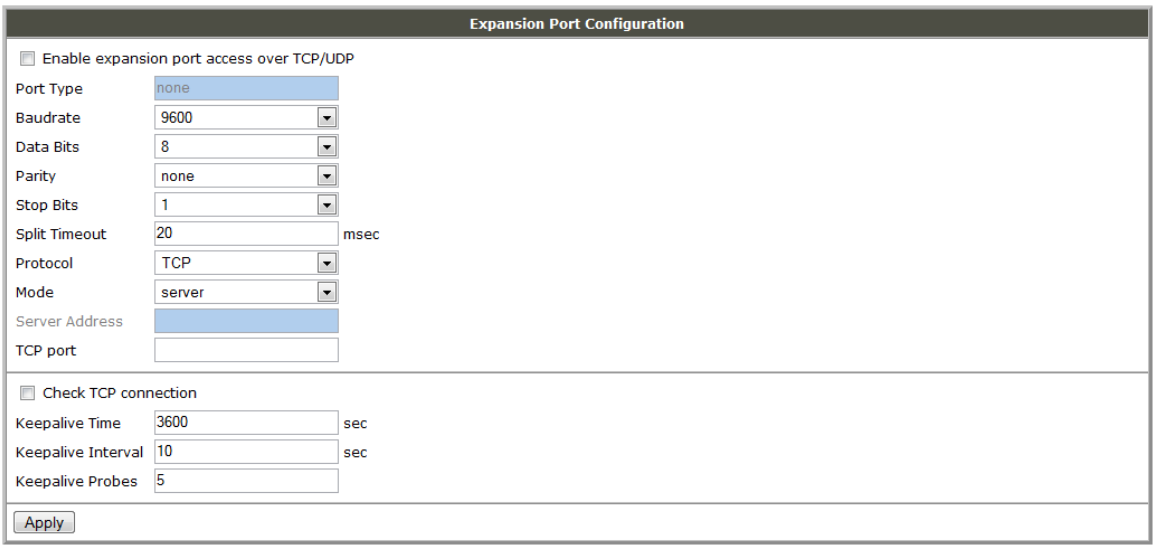
AT+CMGR=1 Enter
+CMGL: <Index>, <Status>,<Absendernummer>, <Datum>,<Zeit>
Text der SMS Nachricht.
+CMGL: 1,“REC READ“,“+420721123456“, ,“08/01/12, 9:48:04+04“
Hello World!

Die empfangene SMS Nachricht kann mit dem Befehl AT+CMGD=<Index> gelöscht werden.

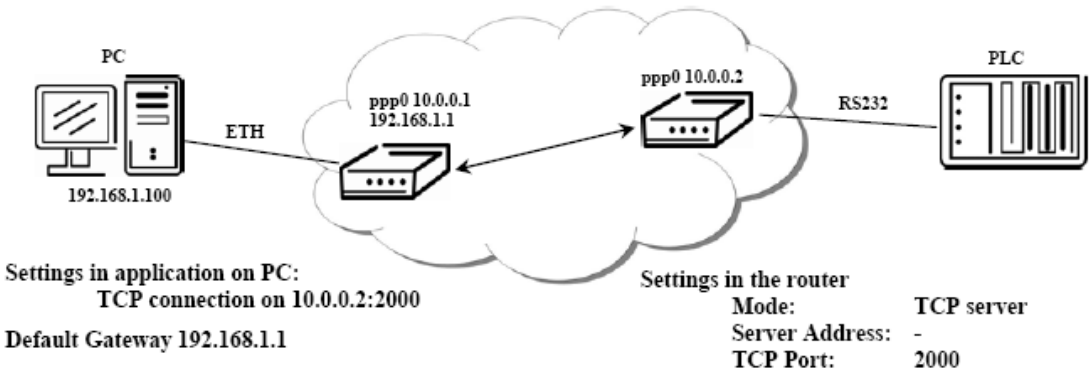
AT+CMGD=1 Enter
OK

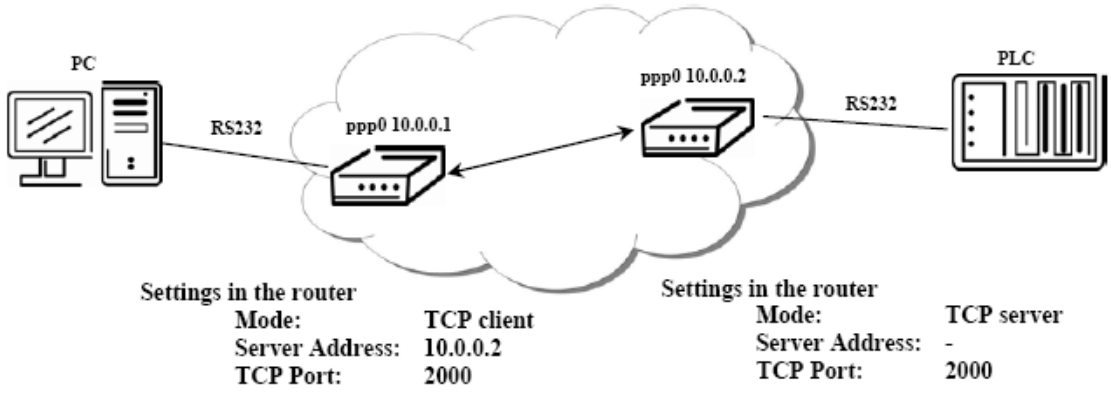
5.20. *Konfiguration des Erweiterungsanschlusses PORT1*

Die Konfiguration des Erweiterungsanschlusses PORT1 kann durch die Auswahl der Option External Port im Menü aufgerufen werden. Im Fenster können die Geschwindigkeit der Kommunikation *(Baudrate)*, die Anzahl der Datenbits *(Data Bits)*, die Parität *(Parity)*, die Anzahl der Stoppbits *(Stop Bits)*, das Protokoll *(Protocol)* definiert und der Modus der Tätigkeit *(Mode)* gewählt werden.
Split Timeout stellt die Zeit für die Zerteilung der Nachricht ein. Wird beim Empfang eine Lücke zwischen zwei Zeichen, die länger als der Wert des Parameters in Millisekunden ist, erkannt, wird der Empfang als fehlerhaft angezeigt und es folgt das Aufsuchen vom neuen Anfang der Nachricht.
Im Modus des TCP Servers ist es notwendig, den TCP Anschluss einzugeben, an dem der Router die ankommenden Anforderungen auf TCP Verbindung anhört. Im Modus des TCP Klienten ist es notwendig die Serveradresse und den TCP Zielanschluss einzugeben.
Ist die Option *Check TCP Connection* angekreuzt, wird die Kontrolle der aufgebauten TCP Verbindung aktiviert. Im Fenster können die Zeit, nach der die Kontrolle der Verbindung erfolgt (Keepalive Time), die Zeit der Antwortabwartung *(Keepalive Interval)* und die Versuchsanzahl *(Keepalive Probes)* definiert werden.
Die Änderungen der Einstellungen wirken sich nach Betätigung der Taste Apply aus.



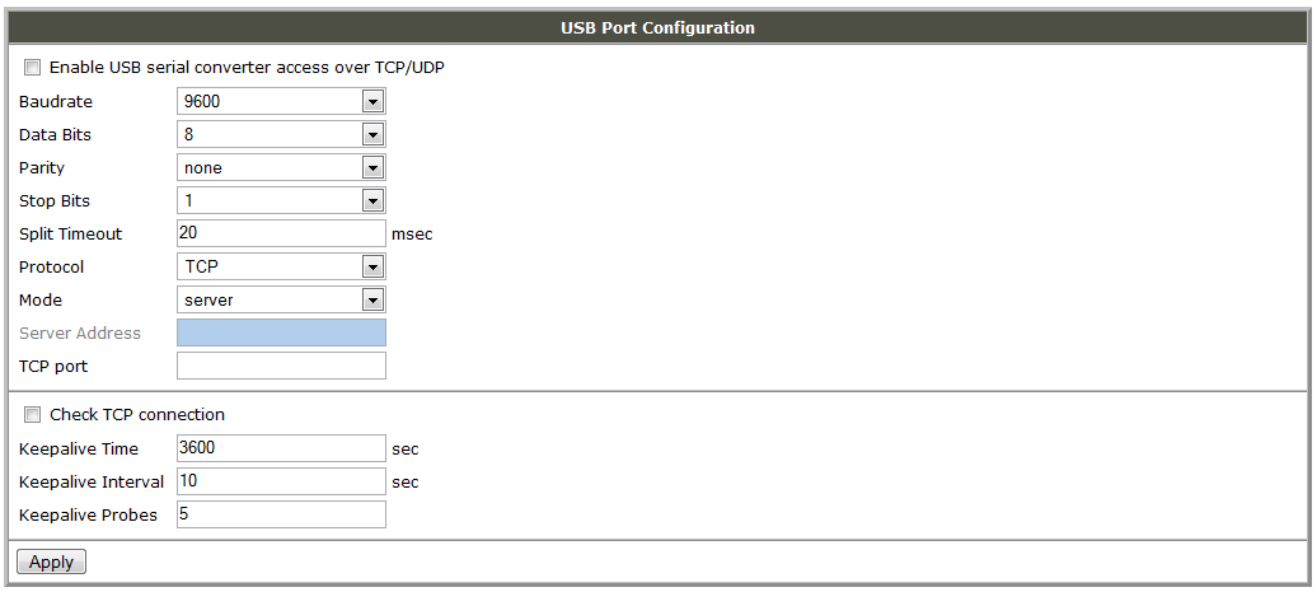
Beispiel für die Konfiguration des Erweiterungsanschlusses:



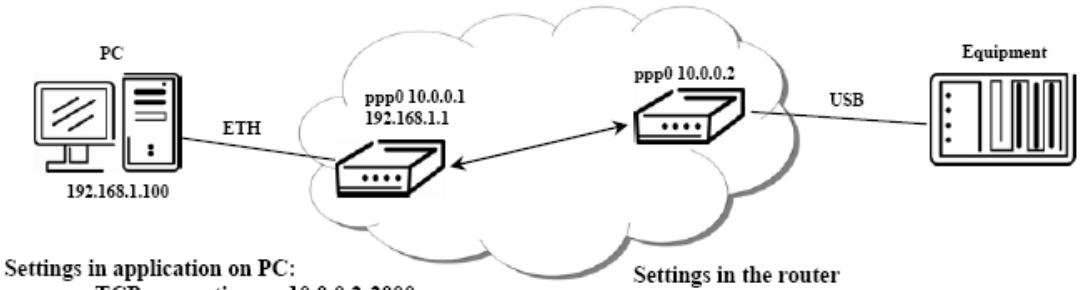


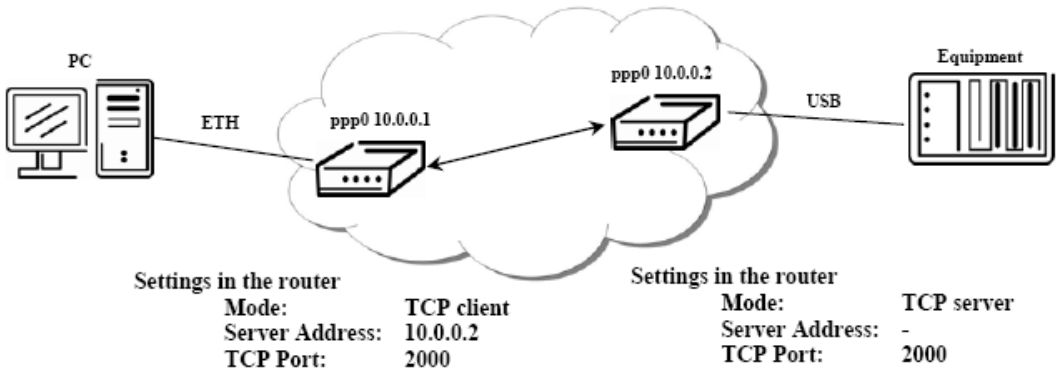
5.21. *Konfiguration des USB Anschlusses*

Die Konfiguration vom USB Anschluss kann durch Auswahl der Option *USB Port* im Menü aufgerufen werden. Im Fenster können die Geschwindigkeit der Kommunikation (*Baudrate*), die Anzahl der Datenbits (*Data Bits*), die Parität (*Parity*), die Anzahl der Stoppbits (*Stop Bits*), das Protokoll (*Protocol*) definiert und der Modus der Tätigkeit (*Mode*) gewählt werden. Split Timeout stellt die Zeit für die Zerteilung der Nachricht ein. Wird beim Empfang eine Lücke zwischen zwei Zeichen, die länger als der Wert des Parameters in Millisekunden ist, erkannt, wird der Empfang als fehlerhaft angezeigt und es folgt das Aufsuchen vom neuen Anfang der Nachricht.
Im Modus *TCP Server* ist es notwendig, den TCP Anschluss einzugeben, an dem der Router die ankommenden Anforderungen auf die TCP Verbindung anhört. Im Modus *TCP Client* ist es notwendig, die Serveradresse und den TCP Zielanschluss einzugeben.
Ist die Option *Check TCP Connection* angekreuzt, wird die Kontrolle der aufgebauten TCP Verbindung aktiviert. Im Fenster können die Zeit, nach der die Kontrolle der Verbindung erfolgt *(Keepalive Time)*, die Zeit der Antwortabwartung *(Keepalive Interval)* und die Versuchsanzahl *(Keepalive Probes)* definiert werden.
Die Änderungen der Einstellungen wirken sich nach Betätigung der Taste *Apply* aus.



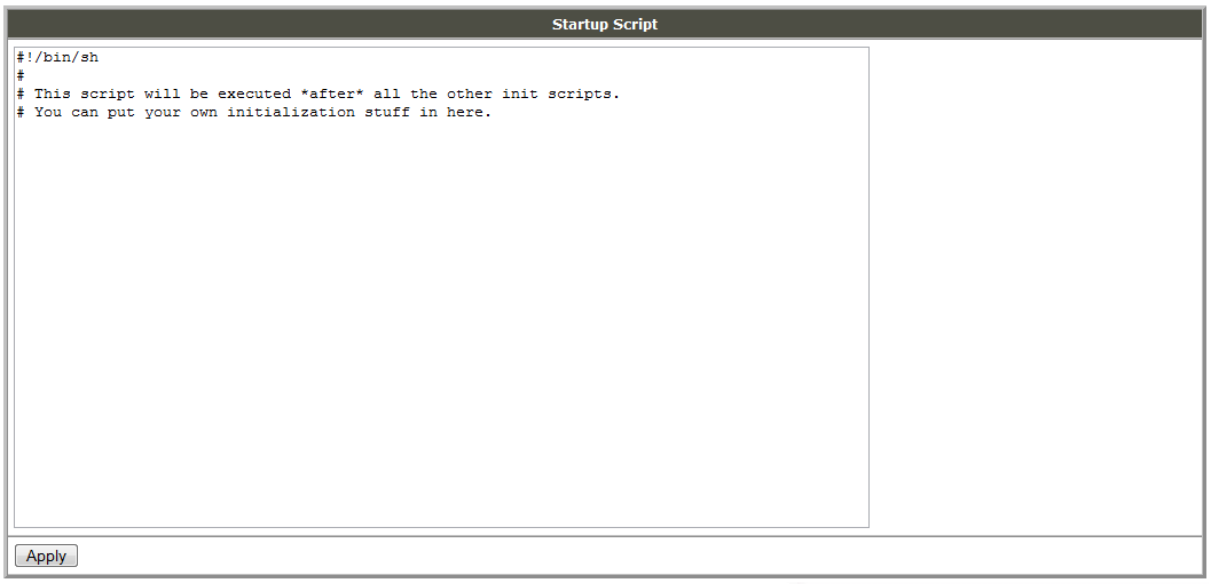
Beispiel für die Konfiguration des USB Anschlusses





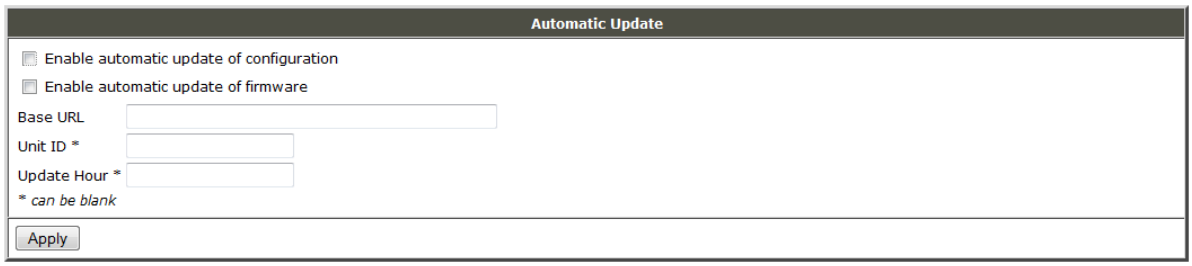
5.22. *Konfiguration des Startskripts*

Im Fenster *Startup Script* ist es möglich eigene Skripten zu erstellen, die nach den Initialisierungsskripten gestartet werden. Bei der Erstellung der Sicherheitskopie sowie bei der Wiederherstellung der Konfiguration werden weder Sicherheitskopien der Skripten erzeugt, noch die Skripten wiederhergestellt.
Die Änderungen der Einstellungen wirken sich nach Betätigung der Taste *Apply* aus.


Startup Script
#!/bin/sh
#
This script will be executed *after* all the other init scripts.
You can put your own initialization stuff in here.
Apply

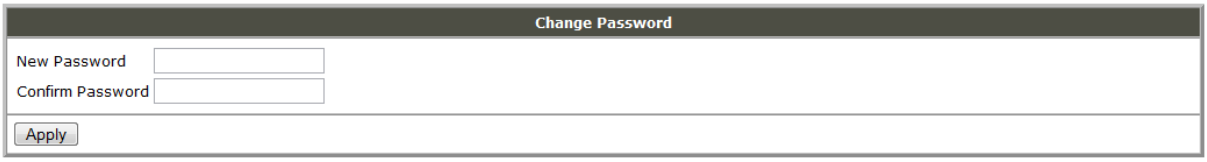
5.23. *Konfiguration der automatischen Aktualisierung der Einstellungen*

Die Konfiguration der automatischen Aktualisierung der Routereinstellungen kann im Menü durch die Auswahl der Option *Automatic Update* aufgerufen werden. Diese Option ermöglicht, dass der Router selbst die Konfiguration oder die aktuelle Firmware vom Server, wo die Konfiguration oder die Firmware gespeichert wird, automatisch herunterlädt. Durch das Ankreuzen der Option *Enable Automatic Update of Configuration* ist es möglich die automatische Aktualisierung der Routereinstellungen freizugeben. Mit dem Parameter *Enable automatic update of firmware* ist es möglich die automatische Aktualisierung der Router-Firmware freizugeben. Mit dem Parameter *Base URL* ist es möglich, den Grundteil der Domäne oder IP Adresse einzugeben, von der die Routerkonfiguration heruntergeladen wird. Diese Adresse wird dann mit dem Inhalt des Parameters *Unit ID*, oder wenn das Feld *Unit ID* nicht ausgefüllt ist, mit der MAC Adresse ergänzt. Die Bezeichnung der heruntergeladenen Datei setz sich aus dem Parameter *Base URL*, der Hardwareadresse MAC der ETH0 Schnittstelle des Routers und aus dem Suffix *cfg* zusammen. Die Hardwareadresse MAC und das Suffix cfg werden automatisch hinzugefügt, es ist nicht erforderlich, diese Daten irgendwo auszufüllen. Mit dem Parameter *Unit ID* kann die sachliche Bezeichnung der heruntergeladenen Datei definiert werden, die auf den Router heruntergeladen wird. Falls dieser Parameter werdendet wird, wird die Hardwareadresse MAC in der Bezeichnung der heruntergeladenen Datei nicht benutzt.
Die automatische Aktualisierung der Konfiguration erfolgt 5 Minuten nach dem Einschalten des Routers und dann alle 24 Stunden, oder es ist möglich mit dem Parameter *Update Hour* die Stunde (im Bereich von 1–24) einzustellen, wann die Aktualisierung durchzuführen ist. Besteht an der eingegebenen URL eine abweichende Konfiguration als im Router, nimmt der Router diese Konfiguration auf und danach führt er einen erneuten Start durch.
Die Änderungen der Einstellungen wirken sich nach Betätigung der Taste *Apply* aus.



5.24. *Änderung des Zutrittspasswortes*

Das Dialogfenster zur Passwortänderung kann durch die Auswahl der Option *Change Password* im Menü aufgerufen werden. Das neue Passwort wird nach der Betätigung der Taste *Apply* gespeichert.
In der Grundeinstellung des Routers ist das Passwort auf die Ausgangsform Root eingestellt. Um die höhere Sicherheit des vom Router verwalteten Netzes sicherzustellen, wird empfohlen dieses Passwort zu ändern.

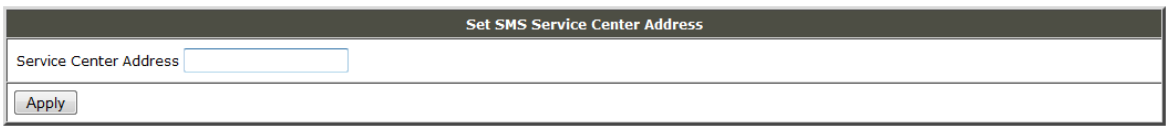


5.25. *Einstellung der internen Uhr*

Die einmalige Einstellung der internen Routeruhr kann durch die Auswahl der Option *Set Real Time Clock* im Menü aufgerufen werden. Die Uhr wird in Abhängigkeit vom eingegebenen NTP Server nach Betätigung der Taste *Apply* eingestellt.

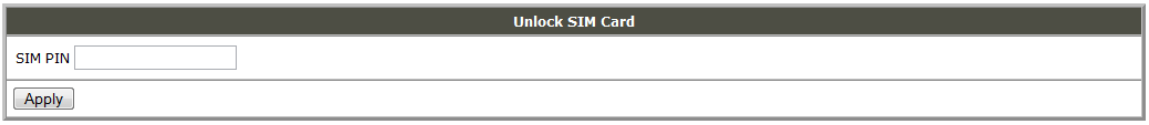
5.26. *Einstellung des SMS Zentrums*

In einigen Fällen ist es notwendig, die Telefonnummer vom SMS Zentrum einzustellen, um die SMS In einigen Fällen ist es notwendig die Telefonnummer vom SMS Zentrum einzustellen, um die SMS Benutzernachrichten auszusenden. Der Parameter muss bei den SIM Karten, die die Telefonnummer des SMS Zentrums vom Netzbetreiber eingestellt haben, nicht eingestellt werden. Die Telefonnummer kann ohne der internationalen Vorwahl xxx xxx xxx oder mit der internationalen Vorwahl +420 xxx xxx xxx angeführt werden.



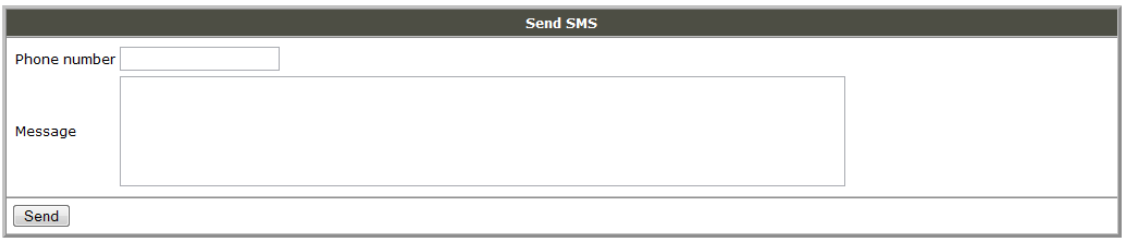
5.27. *Erschließung der SIM Karte*

Die Möglichkeit der Erschließung der SIM Karte ist unter der Option *Unlock SIM Card* angeführt. Ist die in den Router eingelegte SIM Karte mit einem PIN geschützt, wird der PIN (vierstellige Nummer) in das Feld *SIM PIN* eingetragen, die SIM Karte wird durch das Anklicken der Taste Apply erschlossen.



5.28. *Versenden einer SMS Nachricht*

Das Versenden einer SMS Nachricht ist im Fenster *Send SMS* möglich. Nach der Eingabe der Telefonnummer des Empfängers *(Phone Number)* sowie des Textes der SMS Nachricht *(Message)* wird die Nachricht mit der Taste *Send* abgesandt.



Versenden der SMS Nachricht über die HTTP Abfrage ist dann im Format:

GET /send_exec.cgi?phone=%2B**420712345678**&message=**Test** HTTP/1.1
Authorization: Basic cm9vdDpyb290

Die HTTP Abfrage wird in die TCP Verbindung am Anschluss 80 des Routers gesandt, der anschließend eine SMS im Format Test auf die eingegebene Nummer 420712345678 sendet. Die Autorisierung ist im Format „User:Password" verschlüsselte BASE64, das Beispiel ist für root:root.

5.29. *Erstellung der Sicherheitskopie der Konfiguration*

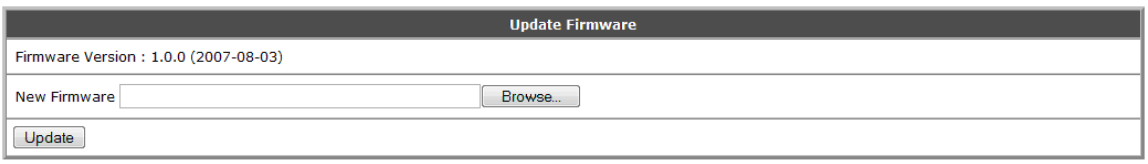
Es ist möglich die Modemkonfiguration mittels der Option *Backup Configuration* zu speichern. Nach dem Anklicken ist es möglich das Zielverzeichnis auszuwählen, wo die Konfigurationsdatei des Routers gespeichert wird.

5.30. *Wiederherstellung der Konfiguration*

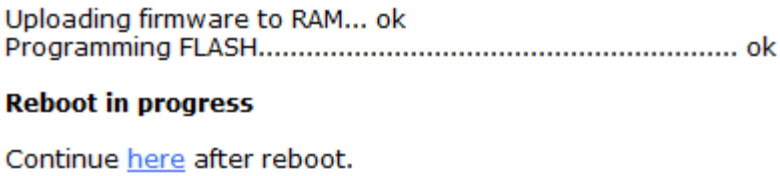
Falls die Routerkonfiguration wiederher hergestellt werden soll, ist es möglich die Konfigurationsdatei in der Option *Restore Configuration* mittels der Taste *Durchsuchen* zu wählen.

5.31. *Aktualisierung der Firmware*

Informationen über die Firware-Version und die Anweisungen zur Aktualisierung können durch die Auswahl der Option Update Firmware im Menü aufgerufen werden. Die neue Firmware wird in der Option Durchsuchen eingelesen und wird durch die anschließende Betätigung der Taste Update aktualisiert.



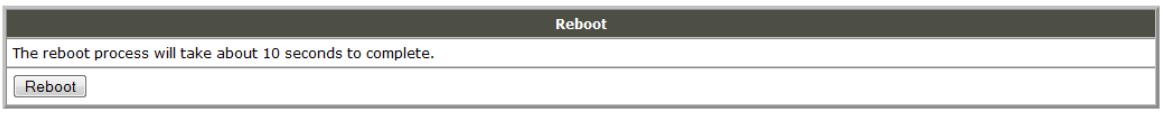
Nach erfolgreicher Aktualisierung der Firmware wird der folgende Auszug ausgeschrieben.



Dieser Auszug informiert über die Programmierung des FLASH Speichers.
Bei der Aktualisierung der Firmware ab Version 1.0.5 bleiben sämtliche Einstellungen samt der IP Adresse erhalten. Bei der Aktualisierung älterer Firmware als der Version 1.0.5 wird die eigene Router-Adresse auf 192.168.1.1 eingestellt (ein Verweis wird hier angeboten) und sämtliche Werte werden auf die Ausgangswerte eingestellt. Die Gesamtzeit der Aktualisierung beträgt etwa drei Minuten. Im Verlauf der Aktualisierung der Firmware muss eine ununterbrochene Stromversorgung sichergestellt werden. Die Fernaktualisierung wird mit Rücksicht auf die GPRS Verbindung nicht empfohlen, es könnte zur Beschädigung des Routers kommen.

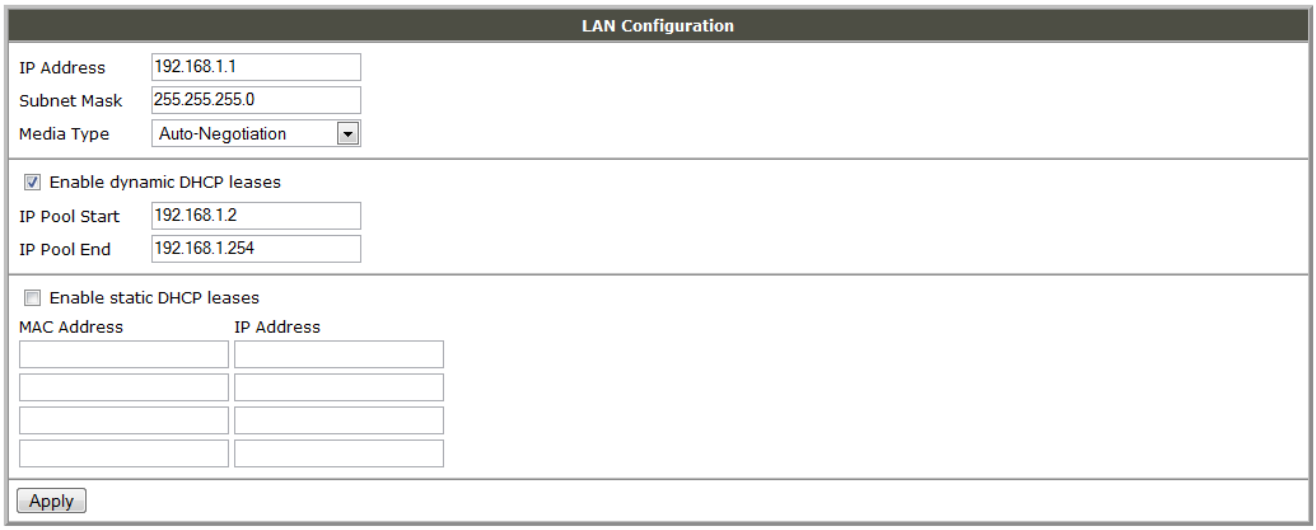
5.32. *Restart*

Der erneuter Start des Routers kann durch die Auswahl der Option Reboot im Menü und durch die anschließende Betätigung der Taste *Reboot* aufgerufen werden.

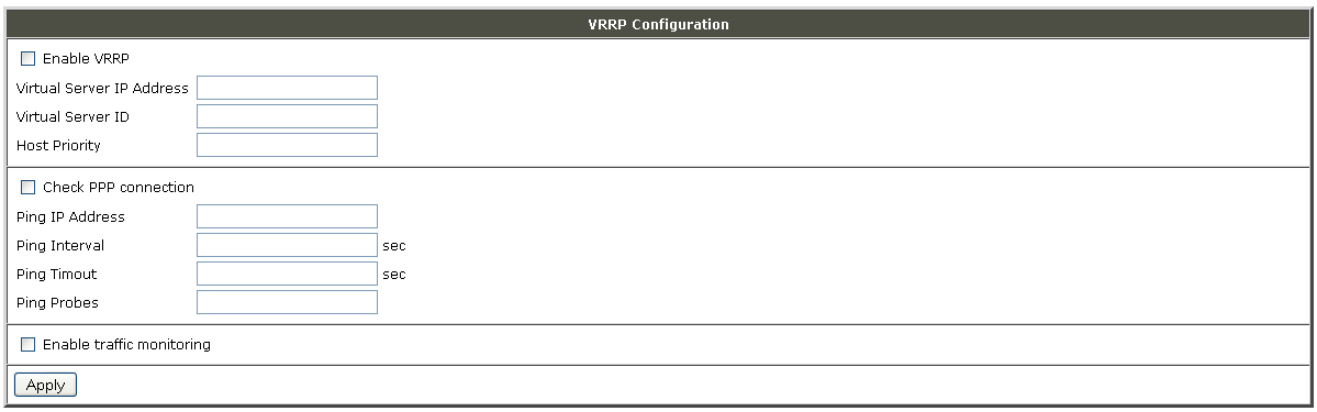


5.33. *Standardeinstellung (Parameter des Herstellerwerkes)*

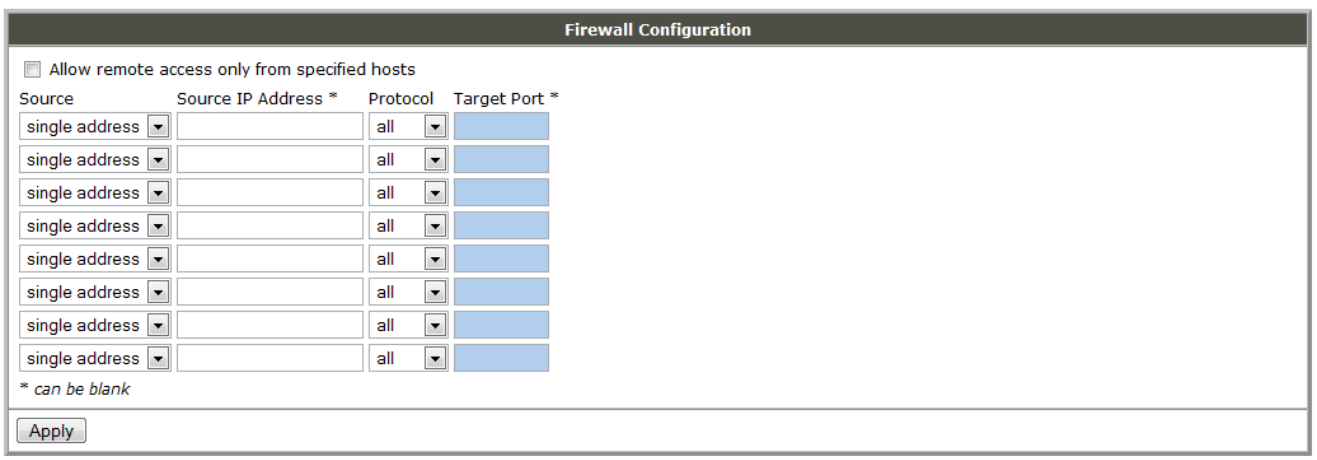
5.33.1. LAN Configuration



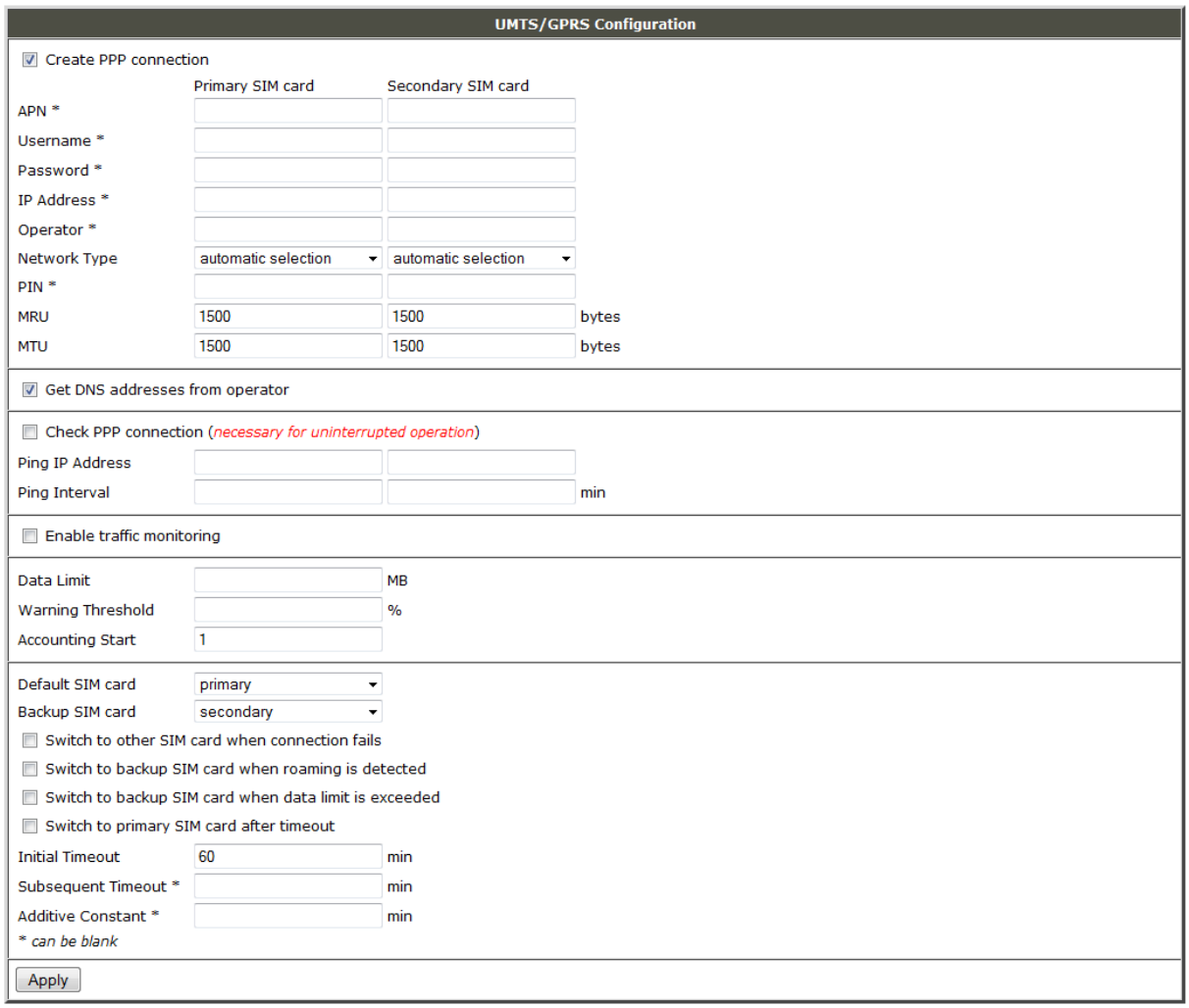
5.33.2. VRRP Configuration



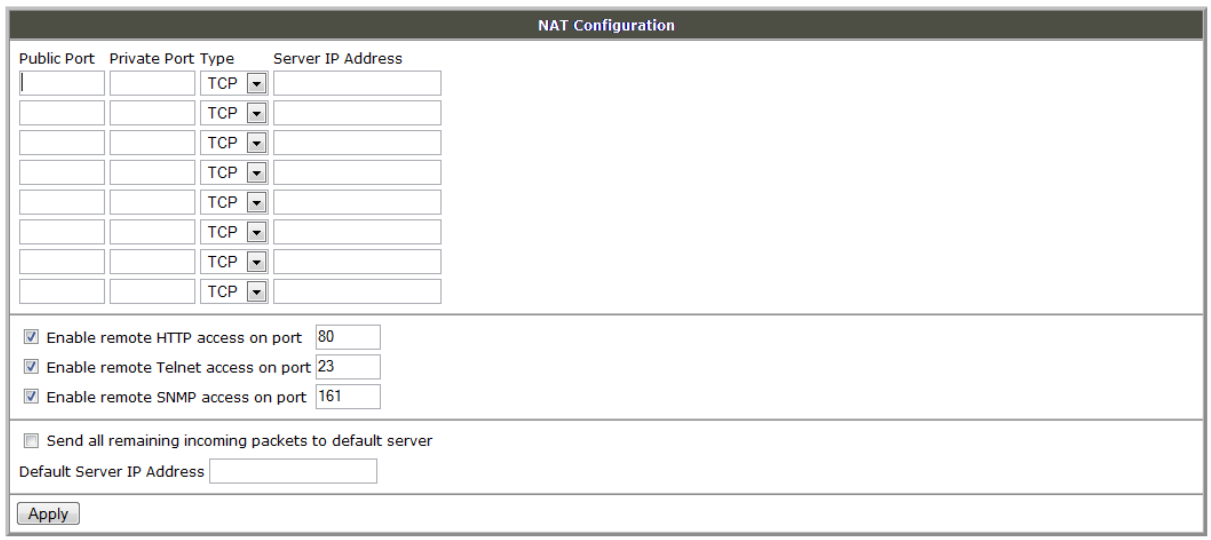
5.33.3. Firewall Configuration



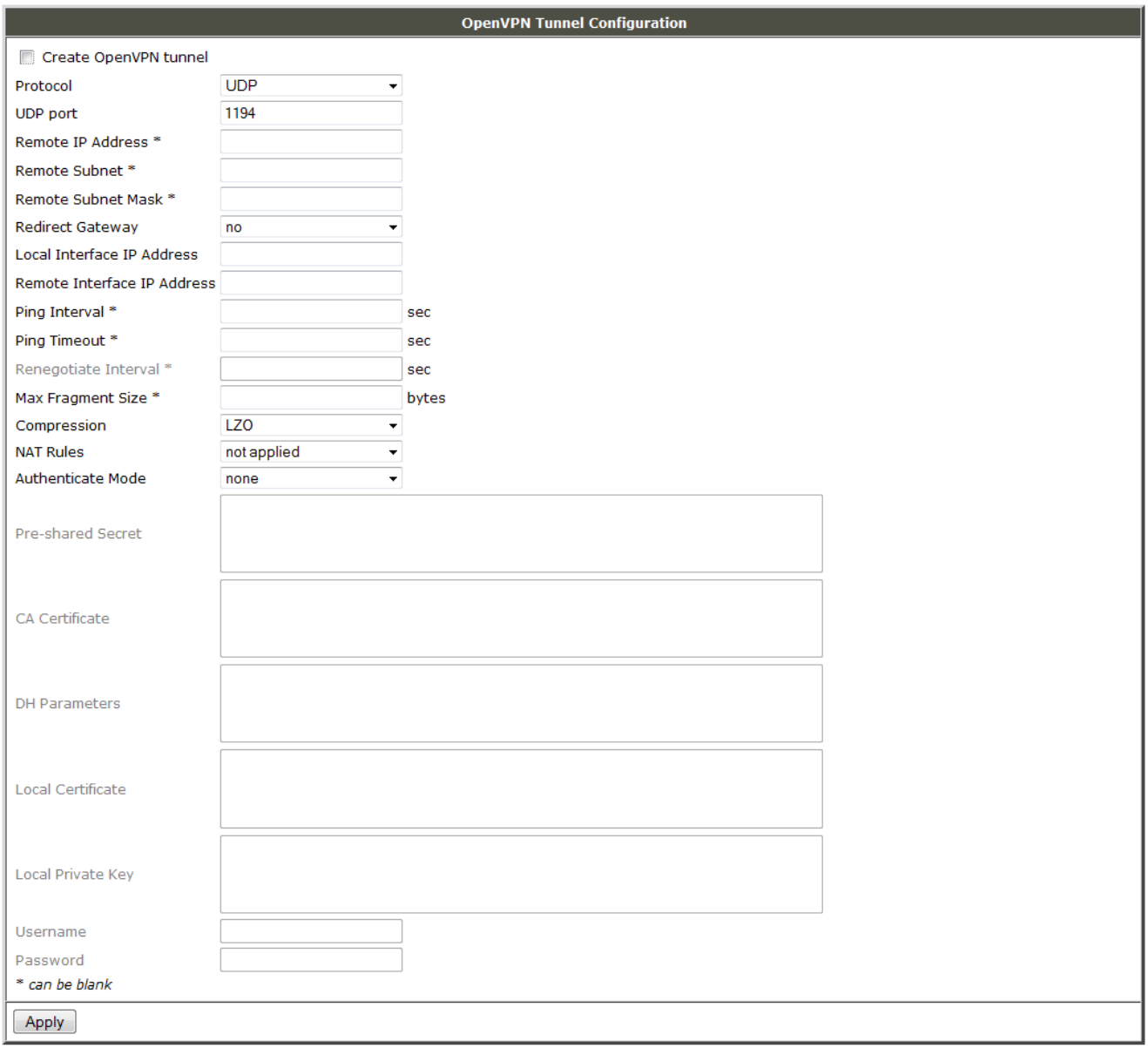
5.33.4. UMTS/GPRS Configuration



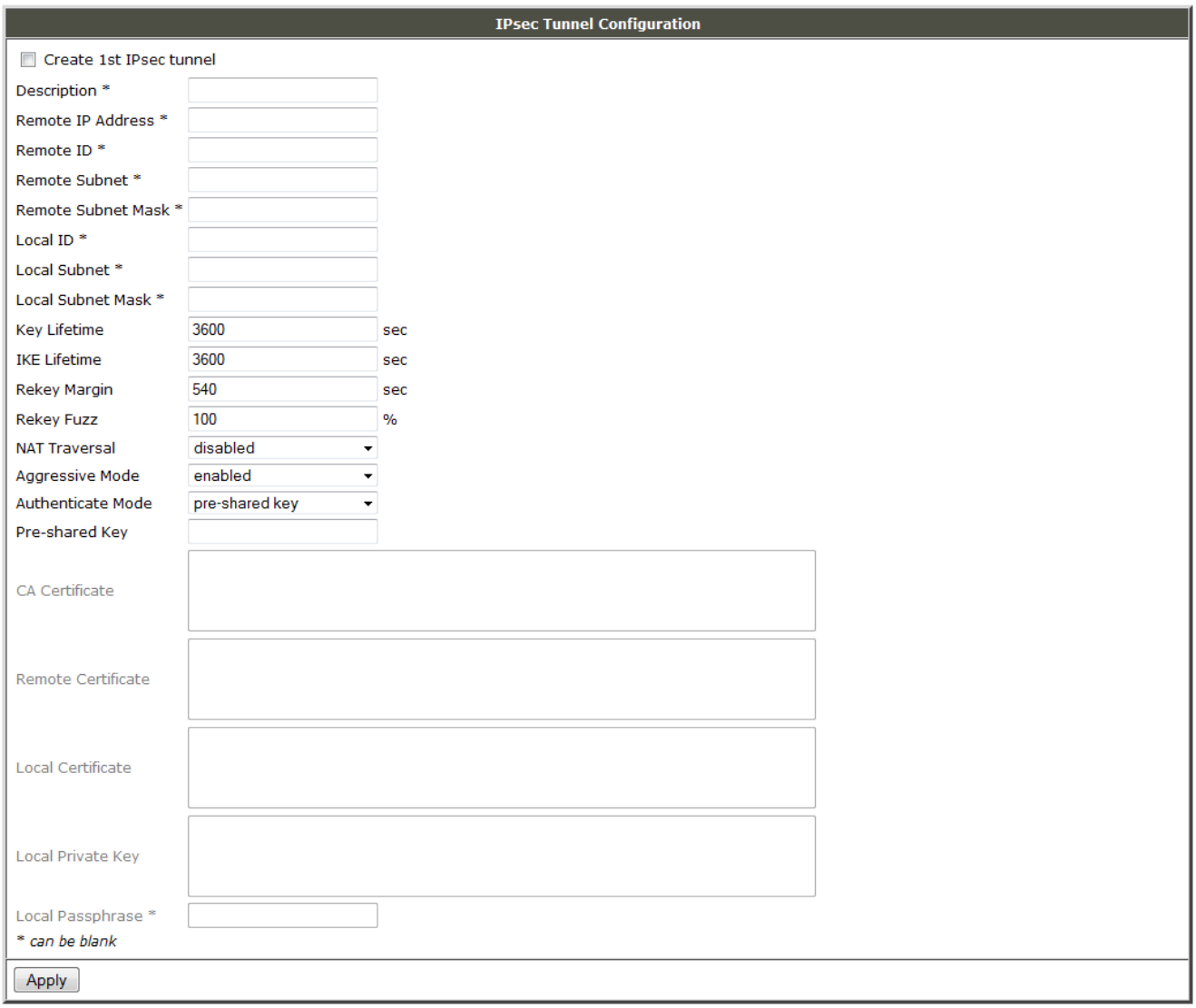
5.33.5. NAT Configuration



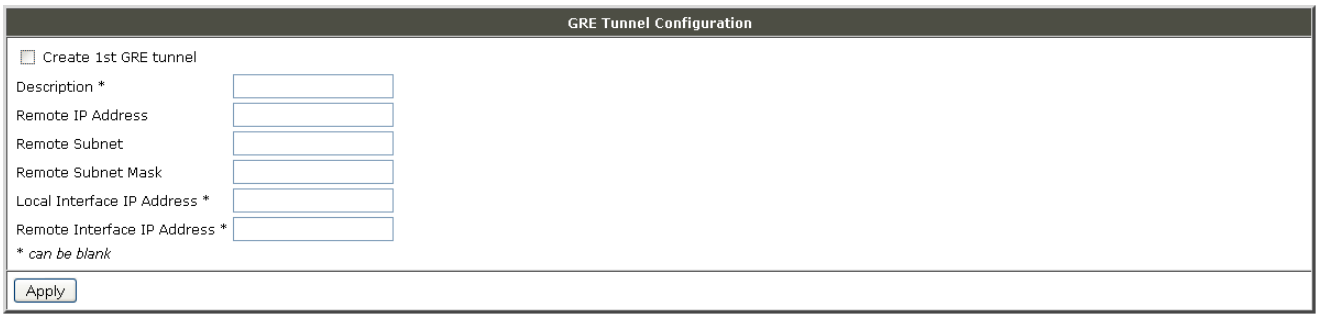
5.33.6. OpenVPN Tunnel Configuration



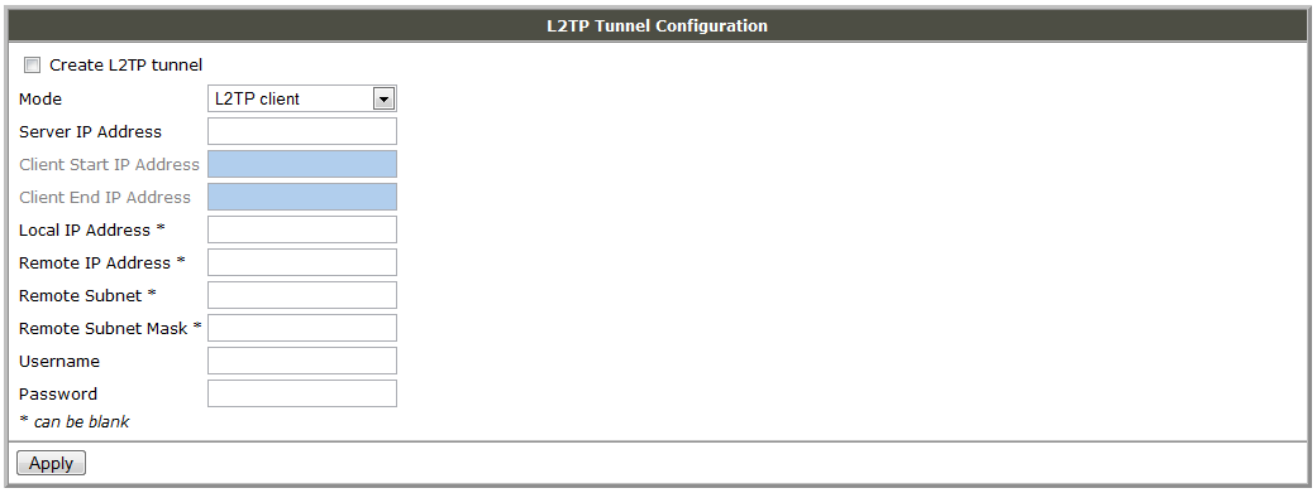
5.33.7. IPsec Tunnel Configuration



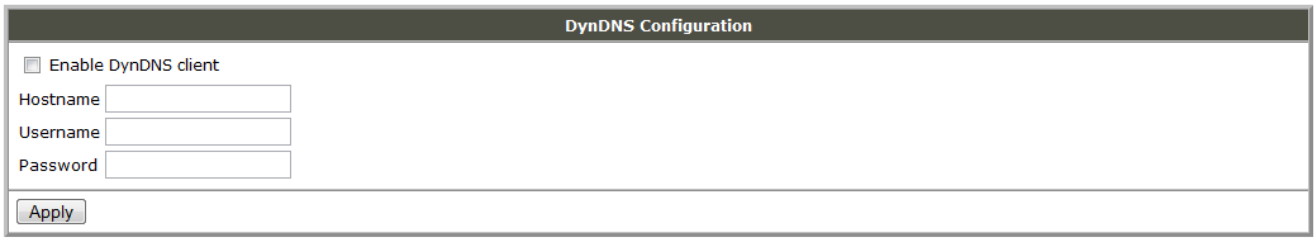
5.33.8. GRE Tunnels Configuration



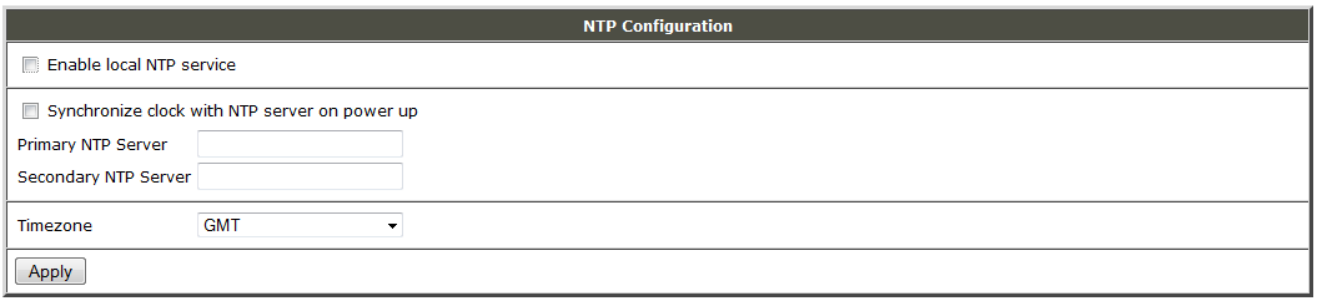
5.33.9. L2TP Tunnel Configuration



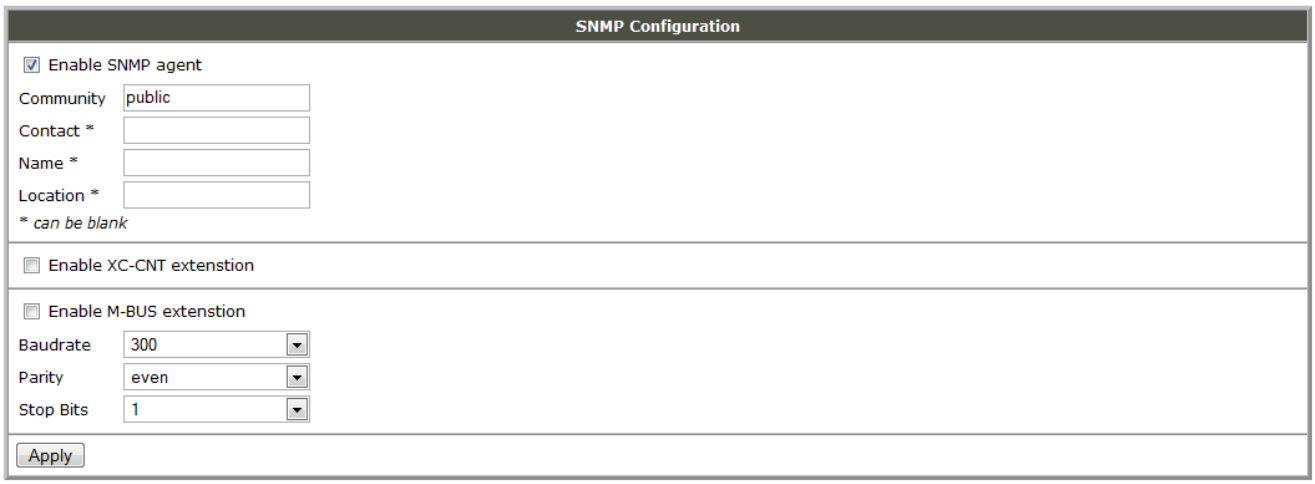
5.33.10. DynDNS Configuration



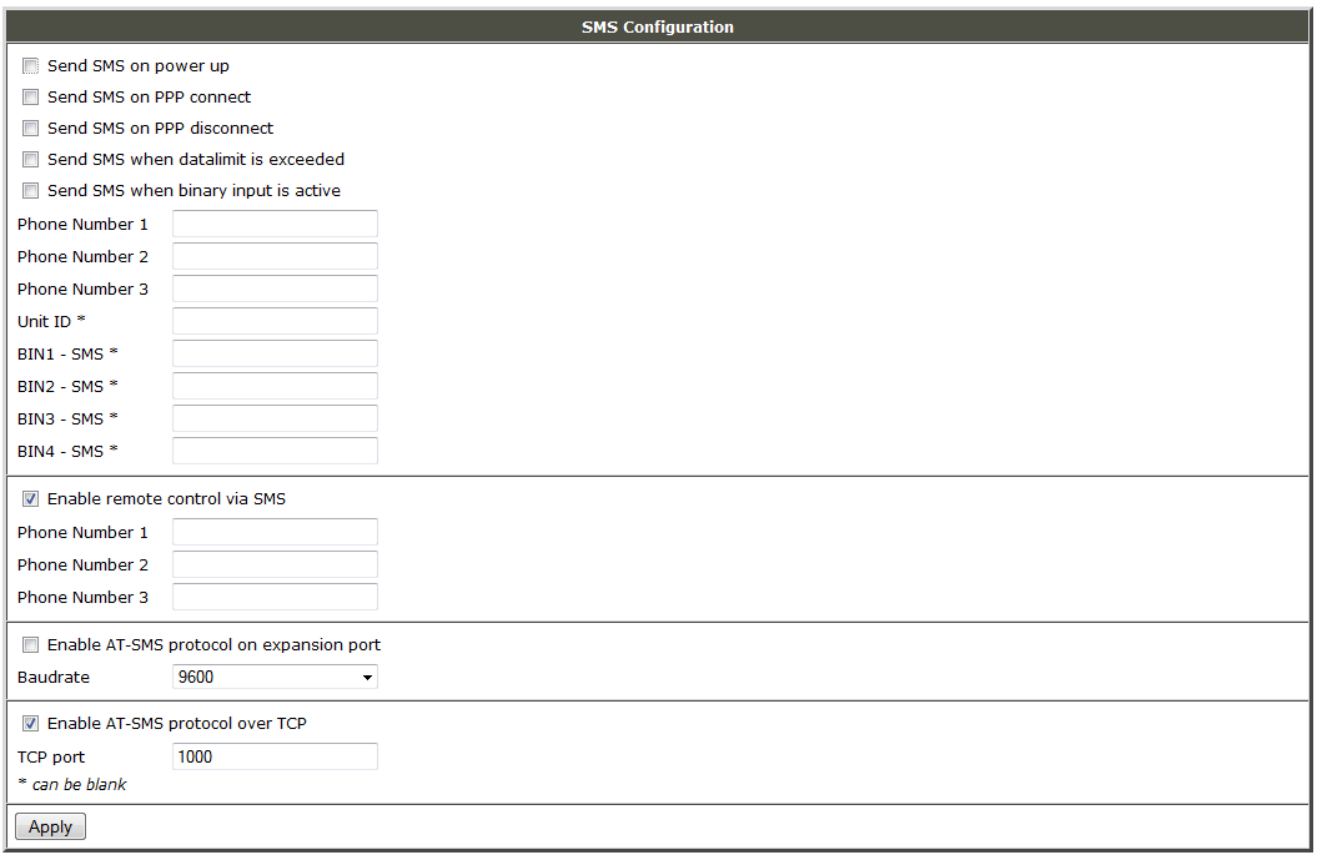
5.33.11. NTP Configuration



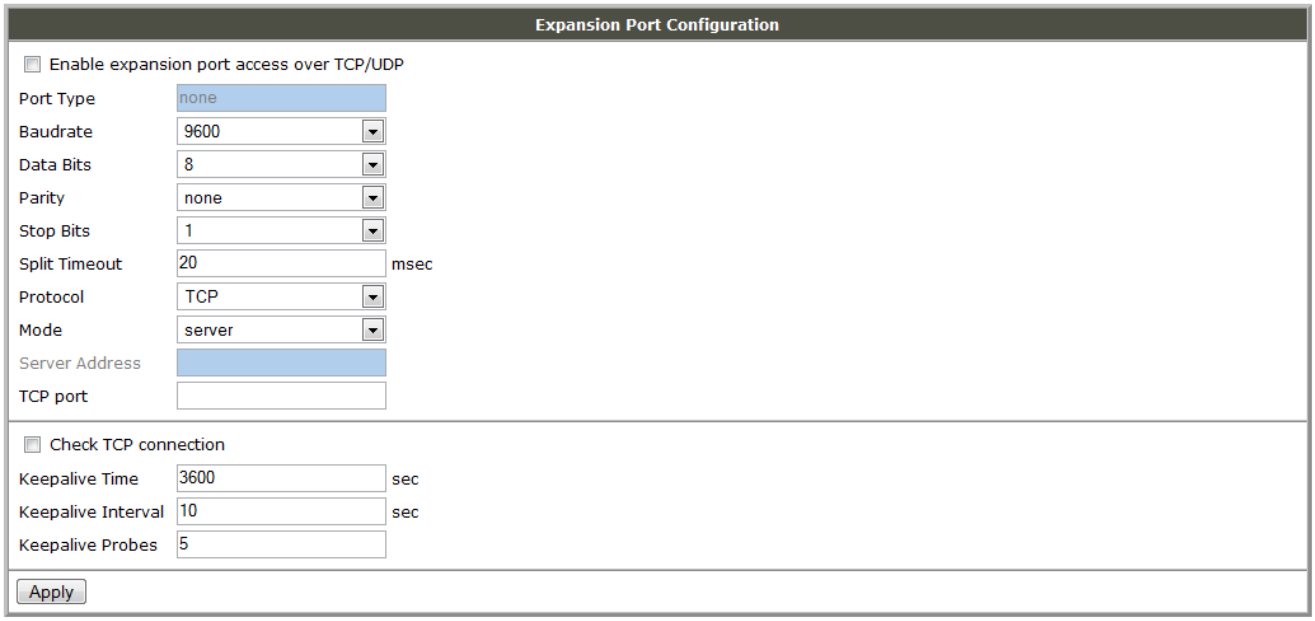
5.33.12. SNMP Configuration



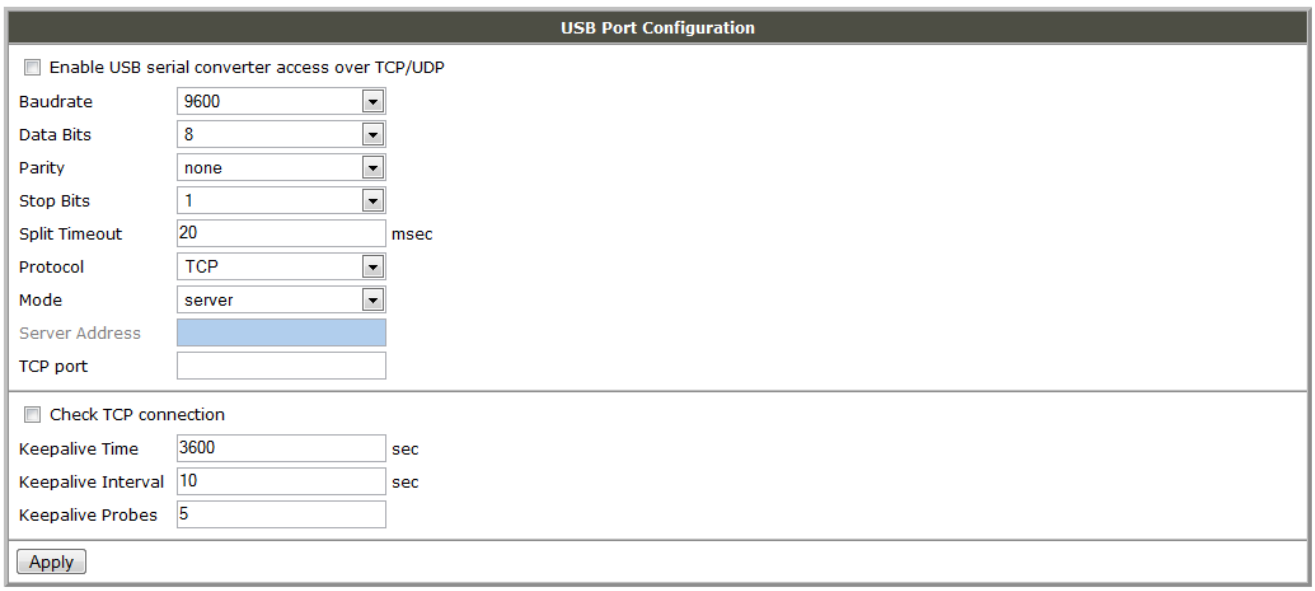
5.33.13. SMS Configuration



5.33.14. Expansion Port Configuration



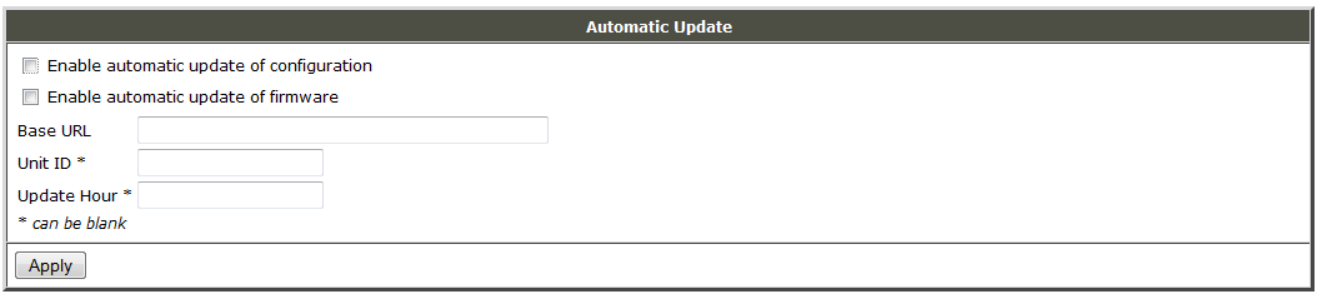
5.33.15. USB Port Configuration



5.33.16. Startup script

Startup Script
#!/bin/sh
#
This script will be executed *after* all the other init scripts.
You can put your own initialization stuff in here.
Apply

5.33.17. Automatic Update



6. Einstellung der Konfiguration über Telnet

Vorsicht! Ohne eingelegte SIM Karte kann der Router nicht betrieben werden. Die eingelegte SIM Karte muss die GPRS Übertragungen aktiviert haben. Die SIM Karte legen Sie dann ein, wenn der Router abgeschaltet ist.
Zur Zustandsüberwachung, Konfiguration und Verwaltung des Routers steht die Telnet Schnittstelle zur Verfügung. Nach der Eingabe der IP Adresse des Routers in die Telnet Schnittstelle ist es möglich, die Konfiguration mittels der Befehle durchzuführen. Die IP Ausgangsadresse des Routers lautet 192.168.1.1. Die Konfiguration kann nur der Benutzer „Root" mit dem Ausgangspasswort „Root" vornehmen.

Für Telnet bestehen folgende AT Befehle:

Befehl	Beschreibung
cat	Auszug aus dem Dateiinhalt
cp	Datei kopieren
date	Anzeige / Änderung der Systemzeit
df	Anzeige der Informationen über das Dateisystem
dmesg	Anzeige der Diagnostikmeldungen von Kernel
echo	Auszug der Zeichenkette
free	Anzeige der Informationen über den Speicher
gsmat	Versand von AT Befehlen
gsminfo	Anzeige der Informationen über die Signalqualität
gsmsms	SMS Versand
hwclock	Anzeige / Änderung der Zeit im RTC Kreis
ifconfig	Anzeige / Änderung der Schnittstellenkonfiguration
ip	Anzeige / Änderung der Richttabelle
iptables	Anzeige / Anpassung der Regel für den Net Filter
kill	Prozessunterbindung
killall	Prozessunterbindung
ln	Erstellung der Verknüpfung
ls	Auszug aus dem Verzeichnisinhalt
mkdir	Verzeichniserstellung
mv	Dateiverschiebung
ntpdate	Synchronisierung der Systemzeit mit NTP Server
passwd	Passwortänderung
ping	ICMP ping
ps	Anzeige der Informationen über Prozesse
pwd	Auszug aus dem aktuellen Verzeichnis
reboot	Restart
rm	Dateilöschen
rmdir	Verzeichnis löschen
route	Anzeige / Änderung der Richttabelle
service	Dienststart / -stopp
sleep	Pause für die vorgegebene Sekundenanzahl
slog	Anzeige des System Log
tail	Anzeige des Dateiendes
tcpdump	Überwachung des Netzbetriebs
touch	Dateierstellung / Aktualisierung des Dateizeitstempels
vi	Texteditor

7. Mögliche Probleme

Bei manchen Netzkarten kann es vorkommen, dass der Router nicht angeschlossen werden kann. Dieses Problem kann durch folgende Schritte gelöst werden:

- durch die anuelle Auswahl der Geschwindigkeit der Kommunikation von 10 MB/s in den Eigenschaften der Netzkarte,
- durch den Anschluss des Routers über Switch,
- durch das Starten des Computers erst nach dem Beenden des Startens des Routers.

8. Literatur

[1] Cinterion**: HC25_ATC_V01.200** – **AT command Set, 2007**

9. FAQ (oft gestellte Fragen)

Aus dem Internet kann ich das an den Router angeschlossene Gerät nicht erreichen und ich habe NAT eingestellt.

- *Auf dem Gerät müssen Sie die Gateway auf den Router eingestellt haben.*

Der Router führt ein Reset durch, die Verbindung im Ethernet fällt aus.

- *Es ist notwendig, dass Sie eine Antenne im größeren Abstand vom Versorgungsnetzteil benutzen.*

Ich kann den Webserver hinter NAT nicht erreichen.

- *Sie müssen den http Fernzutritt auf dem Router verbieten, die Adresse des Ausgangsservers auf Ihren Webserver einstellen und auf dem Web server Gateway auf den Router einstellen.*

Die PPP Verbindung fällt aus.

- *Überprüfen Sie die Signalstärke. Ist die Signalstärke schwach, benutzen Sie eine bessere Antenne. Haben die Zellen in der näheren Umgebung ein ähnliches Signal, ist es notwendig eine Richtantenne zu benutzen. Die Signalstärke muss im Bereich zwischen -50 dBm und -90 dBm liegen.*
- *Es ist erforderlich Ping einzustellen, damit wird die Verbindung kontrolliert und im Falle eines GPRS Ausfalls erneut aufgebaut.*

Die PPP Verbindung wird nicht aufgebaut.

- *Überprüfen Sie die Einstellung PPP – APN, Name, Passwort und IP Adresse.*
- *Versuchen Sie den PIN einzugeben – Kontrollieren Sie, ob die SIM Karte den PIN Code nicht eingestellt hat.*
- *Bei privaten APN ist es geeignet, das Versenden von DNS Servern abzuschalten.*
- *Schalten Sie das System Log ein und beobachten Sie, wo ein Fehler auftritt.*

Die Verbindung im Ethernet fällt aus oder wird nicht aufgebaut.

- *An der Ethernet Schnittstelle des Routers UR5 kann die Autonegotiation abgeschaltet werden und Geschwindigkeit und der Duplex lassen sich manuell einstellen.*

DynDNS funktioniert nicht.

- *Im privaten APN funktioniert es nicht.*
- *Sind die gleiche IP Adresse bei Ihrem kanonischen Namen und die dyna misch zugeteilte Adresse aufgezeichnet, bedeutet es, dass der Netzbetrei ber NAT oder Firewall benutzt.*
- *NAT kann durch Ping an die Adresse von Ihrem beliebigen Server mit ei ner festen IP Adresse und durch die Kontrolle der Adressen des Routers und der Adresse in Ping überprüft werden.*
- *Firewall kann zum Beispiel per Fernzutritt auf die Webschnittstelle über prüft werden.*
- *Der Netzbetreiber teilt die Adresse der DNS Server nicht zu und ohne DNS Server ist es nicht möglich die Verbindung zum Server dyndns.org aufzubauen. Im System Log wird diese Nachricht abgebildet:*
  - DynDNS daemon started
  - Error resolving hostname: no such file or directory
  - Connect to DynDNS server failed

IPsec Tunnel wird aufgebaut, jedoch die Kommunikation funktioniert nicht.

- *Wahrscheinlich sind die Richtregeln der angeschlossenen Geräte oder der Gateway falsch eingestellt.*

Die FTP Verbindung.

- *Der Router unterstützt den aktiven FTP Modus nicht, benutzen Sie den passiven Modus.*

RS232 funktioniert nicht.

- *Es ist notwendig, das Vorhandensein der Erweiterungsplatte RS232 zu überprüfen.*
- *Überprüfen Sie das Vorhandensein der Platte in der Router Konfiguration* auf der Karte „External Port“, oder überprüfen Sie die Verbindung örtlich *mittels des Telnet Hyperterminals.*

L2TP oder IPSec werden nicht aufgebaut.

- *Überprüfen Sie die Ursache im System Log.*

10. Kundenbetreuung

Aktuelle Informationen über das Produkt finden Sie auf der Seite: www.datasensor.de

Wartung – Tipps:

Mit der SIM Karte sollte man genauso vorsichtig umgehen, wie mit einer Kreditkarte. Biegen Sie die Karte nicht, schützen Sie die Karte vor Beschädigung und setzen Sie die Karte nicht statischer Elektrizität aus.

Bei der Reinigung des Gerätes verwenden Sie keine aggressiven Chemikalien oder scheu-ernde Reinigungsmittel!

Zulassung

Die Gesellschaft Conel s.r.o. erklärt hiermit, dass das in diesem Handbuch beschriebene Gerät alle Grundanforderungen der Richtlinie 1999/5/EG (R&TTE) für den Betrieb in den Ländern der Europäischen Gemeinschaft erfüllt.

Die Konformitätserklärungen wurden ausgegeben und können beim Hersteller eingesehen werden.

11. Hinweise zur Handhabung von elektrischem Abfall

Dieses Produkt darf nicht in den Haushaltsmüll entsorgt werden. Es ist die Verpflichtung des Benutzers, den so gekennzeichneten Abfall an einer dafür bestimmten Recycling Sammelstelle für elektrische und elektronische Anlagen abzugeben. Das Sortieren und Recyceln von solchem Abfall hilft mit, die Umwelt sauber zu erhalten und stellt eine solche Art des Recyclings sicher, der die menschliche Gesundheit und Umwelt schützt. Weitere Informationen über die Möglichkeiten der Abfallentsorgung zum Recycling erhalten Sie am zuständigen Gemeinde- oder Stadtamt, bei einer sich mit der Abfallwirtschaft beschäftigenden Firma, auf den Webseiten der Sammelsysteme, auf dem Internetportal des Umweltministeriums oder bei der Firma, wo Sie das Produkt gekauft haben.

12. Vorgehensweise bei Reklamationen

Sehr geehrter Kunde,
das von Ihnen gekaufte Produkt wurde beim Hersteller etwaigen Tests unterzogen und vor dem Verkauf wurden alle Funktionen erneut von unserem Techniker überprüft. Sollte bei diesem Produkt trotz aller oben angeführten Maßnahmen eine Störung während der Garantiefrist auftreten, wegen der das Produkt nicht ordnungsgemäß weiter genutzt werden kann, bitten wir Sie, bei der Geltendmachung diese Vorgehensweise bei Reklamationen zu beachten.
Zur Erleichterung eines eventuellen Beanstandungsverfahrens vergewissern Sie sich bei der Produktübernahme, ob der Händler, bei dem Sie das Produkt kaufen, die entsprechenden Stellen des Garantiescheins samt Verkaufsdatum, Stempel und Unterschrift ordentlich ausgefüllt hat.
Diese Vorgehensweise bei Reklamationen bezieht sich auf die eingekauften Produkte.
Diese Vorgehensweise bei Reklamationen bezieht sich nicht auf die geleisteten Dienste.

Garantiefristen für die Produkte

Auf das eingekaufte Gerät, Versorgungsnetzteil, Datenkabel und etwaiges Zubehör wird eine Garantie von 24 Monaten ab Verkaufsdatum gewährt. Der Verkaufstag ist gleichzeitig der Tag der Produktübernahme seitens des Kunden.

Geltendmachung der Reklamation

Die Reklamation ist beim Händler, bei dem der Gegenstand der Reklamation eingekauft wurde, geltend zu machen. Bei der Reklamation legt der Kunde den ordentlich ausgefüllten Garantieschein sowie den kompletten Reklamationsgegenstand vor. Der Reklamationsgegenstand sollte in dem Zustand, der dem Zustand beim Verkauf entspricht, vorgelegt werden.

Hinweis!

Der Händler übernimmt keine Haftung für individuelle Einstellungen oder für die im Reklamationsgegenstand gespeicherten Angaben.
Bei Geltendmachung der Beanstandung ist der Kunde verpflichtet, anzuführen, um welchen Mängel des Beanstandungsgegenstandes es sich handelt, bzw. auf welche Weise sich der Mängel auswirkt, sowie welches Recht aus der Haftung für Mängel er geltend macht.

Erledigung der Reklamation

Je nach Umständen stellt der Händler eine kostenlose Mängelbeseitigung sicher bzw. tauscht den Reklamationsgegenstand gegen ein neues Produkt aus bzw. erledigt die Beanstandung auf eine andere Weise in Übereinstimmung mit dem Bürgerlichen Gesetzbuch und mit dem Verbraucherschutzgesetzt.
Im Moment der Geltendmachung der Reklamation seitens des Kunden und durch die Übernahme des Beanstandungsgegenstands seitens des Händlers wird die Garantiefrist unterbrochen. Die Garantiefrist setzt sich ab dem Tag fort, an dem der Kunde den reparierten Reklamationsgegenstand oder das ausgetauschte einwandfreie Produkt übernommen hat oder bei nicht erfolgter Übernahme seitens des Kunden ab dem Tag, an dem der Kunde verpflichtet gewesen wäre, den reparierten Reklamationsgegenstand oder das ausgetauschte Produkt zu übernehmen. Sollte der Händler im Falle der Geltendmachung eines Garantiemangels den fehlerhaften Reklamationsgegenstand gegen ein neues Produkt (samt dem Austausch der IMEI) austauschen, geht der ursprüngliche Reklamationsgegenstand somit in das Eigentum des Händlers und das neue Produkt in das Eigentum des Käufers über.

Ab der Übernahme des neuen Produkts fängt die neue Garantiefrist an zu laufen. Falls der Händler laut Vereinbarung mit dem Kunden die Reklamation mit dem Austausch des Reklamationsgegenstandes gegen ein einwandfreies Produkt erledigt, geht die neue Garantie auf das Produkt zu Ende, wie folgt:

1. Nach dem Ablauf von 12 Monaten ab dem Tag der Übernahme des neuen Produkts durch den Kunden.
2. An dem Tag, an dem die Garantiefrist für das ursprüngliche Produkt Reklamationsgegenstand) hätte ablaufen sollen, wenn der Austausch des Produkts nicht erfolgt wäre, und zwar am nachfolgenden Tag.
3. Um eine unberechtigte Reklamation handelt es sich dann, falls der beanstandete Produktmangel vom Händler im Rahmen der Reklamation nicht festgestellt wird oder sobald es sich um einen Produktmangel handelt, auf den sich nicht die Garantie im Sinne von Artikel 4 dieser Vorgehensweise bei Reklamationen bezieht.
4. Wird der beanstandete Mangel nicht festgestellt und wird die Funktionstüchtigkeit des Reklamationsgegenstandes dem Kunden vorgeführt, ist der Kunde verpflichtet, die nachweisbaren, im Zusammenhang mit der sachkundigen Begutachtung des beanstandeten Mangels entstandenen Kosten zu erstatten.
5. Falls bei der Überprüfung der Bereichtigung der Reklamation ein Produktmangel festgestellt wird, auf den sich nicht die Garantie (Reparatur außerhalb der Garantie) bezieht, informiert der Händler den Kunden über diese Tatsache und der Kunde teilt dem Händler mit, ob er sich die Beseitigung dieses Mangels für den vom Händler verlangten Preis wünscht. Bezüglich der genauen Reparaturbedingungen außerhalb der Garantiefrist wird eine Niederschrift verfasst, die sowohl vom Kunden als auch vom Händler mit ihren Unterschriften bestätigt wird. Verlangt der Kunde die Reparatur der Mängel außerhalb der Garantiefrist zu den Bedingungen, die ihm der Händler mitteilt, wird das Gerät dann an den Kunden zurückgegeben, wenn der Kunde die nachweisbaren, im Zusammenhang mit der sachkundigen Begutachtung des beanstandeten Mangels entstandenen Kosten erstattet.

Die Garantie bezieht sich nicht auf Mängel, die entstanden sind:

1. durch mechanische Beschädigung (z. B. durch einen Sturz u.s.w.)
2. durch die Anwendung von ungeeigneten bzw. für dieses Produkt nicht empfohlenen Versorgungsnetzteilen sowie vom anderen Zubehör in Verbindung mit der Nutzung des Produkts mit nicht standardmäßigem Zubehör.
3. durch Installation oder durch Benutzung des Produkts im Widerspruch mit der Bedienungsanleitung oder durch die Benutzung des Produkts für andere Zwecke, als bei diesem Typ üblich ist.
4. durch unsachgemäße Handhabung bzw. durch den Eingriff in das Produkt durch eine unbefugte Person oder ein anderes als vom Hersteller zugelassenes Servicecenter.
5. durch Beschädigung infolge von höherer Macht (Hochwasser, Brandfall, u.s.w.) oder infolge von anderen örtlichen Erscheinungen (Sturm, Netzüberspannung u.s.w.).
6. durch Lagerung außerhalb des Temperaturbereiches.
7. durch Benutzung in chemisch aggressiver Umgebung.

Sonstige Reklamationsbedingungen
Für einen Mangel wird nicht die Tatsache gehalten, dass der Reklamationsgegenstand nicht den Parametern entspricht, die für andere analoge Produkttypen gelten. Zur Beurteilung, ob es sich um einen Mangel handelt, sind die in der technischen Dokumentation zum Produkt angeführten Produktparameter maßgebend.
Die Garantie erlischt in dem Falle, dass der Reklamationsgegenstand geändert wird oder wenn die Herstellungsnummer des Reklamationsgegenstandes beschädigt oder auf andere Weise unlesbar ist.

13. Garantieschein

Gerätetyp	
Herstellungsnummer	
Garantiefrist (in Monaten)	
Händler	
Verkaufsdatum	
Stempel des Händlers	

	1	2	3	4	5
Datum der Reklamationsannahme durch den Händler					
Nummer des Reklamationsprotokolls					
Datum der Geräteannahme im Service Center					
Datum der Beendigung der Reperatur im Service Center					
Nummer des Reperaturscheins des Service Centers					
Garantiereperatur	JA - NEIN	JA - NEIN	JA - NEIN	JA - NEIN	JA - NEIN
Neue Herstellungsnummer des Gerätes (IMEI)					
Anmerkungen					
Stempel des Service Centers					